日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００２年　１月　８日

出願番号
Application Number: 特願２００２－００１８４３

[ST.10/C]: [ＪＰ２００２－００１８４３]

出願人
Applicant(s): 株式会社エヌ・ティ・ティ・ドコモ

２００３年　２月１２日

特許庁長官
Commissioner,
Japan Patent Office 太田信一郎

出証番号　出証特２００３－３００６５４４

【書類名】　特許願

【整理番号】　DCMH130548

【提出日】　平成14年 1月 8日

【あて先】　特許庁長官　殿

【国際特許分類】　H04L 9/00

【発明の名称】　配信方法および配信システム

【請求項の数】　19

【発明者】

【住所又は居所】　東京都千代田区永田町二丁目１１番１号　株式会社エヌ・ティ・ティ・ドコモ内

【氏名】　山田　和宏

【発明者】

【住所又は居所】　東京都千代田区永田町二丁目１１番１号　株式会社エヌ・ティ・ティ・ドコモ内

【氏名】　渡邉　信之

【発明者】

【住所又は居所】　東京都千代田区永田町二丁目１１番１号　株式会社エヌ・ティ・ティ・ドコモ内

【氏名】　津田　雅之

【発明者】

【住所又は居所】　東京都千代田区永田町二丁目１１番１号　株式会社エヌ・ティ・ティ・ドコモ内

【氏名】　神谷　大

【発明者】

【住所又は居所】　東京都千代田区永田町二丁目１１番１号　株式会社エヌ・ティ・ティ・ドコモ内

【氏名】　浅井　真生

【発明者】

【住所又は居所】　東京都千代田区永田町二丁目１１番１号　株式会社エヌ

・ティ・ティ・ドコモ内

【氏名】　三浦　史光

【発明者】

【住所又は居所】　東京都千代田区永田町二丁目１１番１号　株式会社エヌ・ティ・ティ・ドコモ内

【氏名】　鷲尾　諭

【発明者】

【住所又は居所】　東京都千代田区永田町二丁目１１番１号　株式会社エヌ・ティ・ティ・ドコモ内

【氏名】　富岡　淳樹

【発明者】

【住所又は居所】　東京都千代田区永田町二丁目１１番１号　株式会社エヌ・ティ・ティ・ドコモ内

【氏名】　川端　博史

【発明者】

【住所又は居所】　東京都千代田区永田町二丁目１１番１号　株式会社エヌ・ティ・ティ・ドコモ内

【氏名】　近藤　隆

【特許出願人】

【識別番号】　392026693

【氏名又は名称】　株式会社エヌ・ティ・ティ・ドコモ

【代理人】

【識別番号】　100098084

【弁理士】

【氏名又は名称】　川▲崎▼　研二

【選任した代理人】

【識別番号】　100111763

【弁理士】

【氏名又は名称】　松本　隆

【手数料の表示】

【予納台帳番号】　038265

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　配信方法および配信システム

【特許請求の範囲】

【請求項１】　アプリケーションを実現するためのソフトウェアを内包した実体ファイルを格納した情報提供サーバ装置と、前記実体ファイルに依存した内容を有し前記実体ファイルの格納位置を示すアプリケーション記述ファイルを格納した情報提供サーバ装置と、前記アプリケーション記述ファイルの格納位置を示す第１の識別情報と前記端末装置が前記ソフトウェアを実行することにより実現されるアプリケーションに与えられた権限を示す権限情報とを内包したセキュリティ記述ファイルを格納した管理サーバ装置とを有し、ファイルの格納位置を通知されると当該ファイルを返送する通信システムが、アプリケーションに与えられた権限に応じた挙動を当該アプリケーションに対して許可する端末装置へ前記セキュリティ記述ファイルを、セキュリティを確保して送信する権限送信過程と、

前記端末装置が、前記権限送信過程にて前記通信システムから送信された前記セキュリティ記述ファイルに内包されている前記第１の識別情報を用いて前記アプリケーション記述ファイルを取得する依存情報取得過程と、

前記端末装置が、前記依存情報取得過程にて取得した前記アプリケーション記述ファイルを用いて前記通信システムから前記実体ファイルを取得するプログラム取得過程と

を有する配信方法。

【請求項２】　前記通信システムはセキュリティの確保された通信路を介して前記セキュリティ記述ファイルを送信することによりセキュリティを確保する

請求項１に記載の配信方法。

【請求項３】　前記通信路は暗号化されている

請求項２に記載の配信方法。

【請求項４】　前記通信路は移動通信網および専用線により実現される

請求項２に記載の配信方法。

【請求項５】　前記通信路は移動通信網および暗号化された通信路により実

現される

請求項２に記載の配信方法。

【請求項６】　前記通信システムが前記セキュリティ記述ファイルを暗号化する暗号化過程と、

前記端末装置が、前記権限送信過程にて前記通信システムから送信された前記セキュリティ記述ファイルを復号する復号過程とを有し、

前記権限送信過程では、前記暗号化過程にて暗号化された前記セキュリティ記述ファイルを前記端末装置へ送信し、

前記依存情報取得過程では、前記端末装置が、前記復号過程にて復号された前記セキュリティ記述ファイルを用いて前記アプリケーション記述ファイルを取得する

請求項１に記載の配信方法。

【請求項７】　前記権限情報は資源の利用に関する制限を示す

請求項１に記載の配信方法。

【請求項８】　前記資源は前記端末装置内部のハードウェア資源である

請求項７に記載の配信方法。

【請求項９】　前記資源は前記端末装置外部の、前記端末装置が使用可能なハードウェア資源である

請求項７に記載の配信方法。

【請求項１０】　前記資源は前記端末装置内部のソフトウェア資源である

請求項７に記載の配信方法。

【請求項１１】　前記資源は前記端末装置外部の、前記端末装置が使用可能なソフトウェア資源である

請求項７に記載の配信方法。

【請求項１２】　前記資源は、前記端末装置が使用可能なネットワーク資源である

請求項７に記載の配信方法。

【請求項１３】　前記権限情報は資源の利用の種類を示す

請求項１に記載の配信方法。

【請求項１４】　前記アプリケーションに対応するアプリケーション記述ファイルは前記アプリケーションを提供する情報提供事業者に対して認証局が与えた秘密鍵で署名されており、かつ、前記アプリケーションに対応するセキュリティ記述ファイルは前記情報提供事業者に対して認証局が与えた公開鍵を内包し、

前記プログラム取得過程では、前記端末装置が、前記依存情報取得過程で取得したアプリケーション記述ファイルの正当性を前記公開鍵を用いて検証し、正当性が検証された場合にのみ、当該アプリケーション記述ファイルを用いて前記通信システムから前記実体ファイルを取得する

請求項１に記載の配信方法。

【請求項１５】　前記アプリケーション記述ファイルおよび前記セキュリティ記述ファイルは、前記管理サーバ装置を管理する管理者が付与するアプリケーション識別子を内包し、

前記プログラム取得過程では、前記端末装置が、前記権限送信過程で前記管理サーバ装置から送信されたセキュリティ記述ファイルに内包されたアプリケーション識別子と前記依存情報取得過程で取得したアプリケーション記述ファイルに内包されたアプリケーション識別子とを比較し、両者が一致した場合にのみ、当該アプリケーション記述ファイルを用いて前記通信システムから前記実体ファイルを取得する

請求項１に記載の配信方法。

【請求項１６】　前記通信システムは、さらに、前記セキュリティ記述ファイルの格納位置を示す第２の識別情報を内包したダウンロード用ファイルを格納した情報提供サーバ装置を有し、

前記通信システムが端末装置へ前記ダウンロード用ファイルを送信する事前送信過程と、

前記端末装置が、前記事前送信過程にて前記通信システムから送信された前記ダウンロード用ファイルを用いて前記セキュリティ記述ファイルの送信を前記通信システムに要求する権限送信要求過程とを有し、

前記権限送信過程では、前記通信システムが、前記権限送信要求過程にて要求された前記セキュリティ記述ファイルを前記端末装置へ送信する

請求項１に記載の配信方法。

【請求項１７】　前記依存情報送信過程にて送信されるセキュリティ記述ファイルの格納位置が前記管理サーバ装置内の場合にのみ前記依存情報取得過程以降の過程を実行する

請求項１に記載の配信方法。

【請求項１８】　前記端末装置は移動機である

請求項１～請求項１７のいずれか一の請求項に記載の配信方法。

【請求項１９】　アプリケーションを実現するためのソフトウェアを内包した実体ファイルを格納した情報提供サーバ装置と、前記実体ファイルに依存した内容を有し前記実体ファイルの格納位置を示すアプリケーション記述ファイルを格納した情報提供サーバ装置と、前記アプリケーション記述ファイルの格納位置を示す第１の識別情報と前記端末装置が前記ソフトウェアを実行することにより実現されるアプリケーションに与えられた権限を示す権限情報とを内包したセキュリティ記述ファイルを格納した管理サーバ装置とを有し、ファイルの格納位置を通知されると当該ファイルを返送する通信システムと、

アプリケーションに与えられた権限に応じた挙動を当該アプリケーションに対して許可する端末装置とを有し、

前記管理サーバ装置は、前記セキュリティ記述ファイルを前記端末装置へ、セキュリティを確保して送信し、

前記端末装置は、前記通信システムから送信された前記セキュリティ記述ファイルに内包されている前記第１の識別情報を用いて前記アプリケーション記述ファイルを取得し、前記アプリケーション記述ファイルを用いて前記通信システムから前記実体ファイルを取得する

配信システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、端末装置にアプリケーションを配信する技術に関する。

【０００２】

【従来の技術】

Ｊａｖａ（登録商標）プログラミング言語に従って記述されたプログラムを実行してＪａｖａ－ＡＰ（Ｊａｖａアプリケーション）を実現する機能を備え、この種のプログラムを含むソフトウェアであるＪａｖａ－ＡＰソフトウェアを、ネットワークを介してダウンロードすることができる移動機が普及している。この種の移動機によるＪａｖａ－ＡＰソフトウェアのダウンロード手順は、ＷＷＷ（World Wide Web）を構成するサーバ装置からＡＤＦ（Application Descriptor File）を取得し、次いでＪａｒ（Java Archive）ファイルを取得するという流れになっている。

【０００３】

ＡＤＦはＪａｒファイルに依存した内容となっており、例えば、Ｊａｒファイルの格納位置を示すＵＲＬ（以後、パッケージＵＲＬ）、Ｊａｒファイルのサイズを示す情報、Ｊａｒファイルの最終変更日時を示す情報等を必須情報として内包している。ＡＤＦを取得した移動機はこのＡＤＦの内容を調べ、ダウンロードしようとしているＪａｖａ－ＡＰソフトウェアを当該移動機にインストール可能であるか否かを判断する。

【０００４】

インストール可能と判断すると、移動機は、ＷＷＷを構成するサーバ装置からパッケージＵＲＬを用いてＪａｒファイルを取得する。Ｊａｒファイルには、Ｊａｖａ－ＡＰソフトウェアが格納されており、Ｊａｒファイルの取得をもってＪａｖａ－ＡＰソフトウェアのダウンロードは完了する。以後、移動機において、当該Ｊａｖａ－ＡＰソフトウェアが起動可能に設定され、当該Ｊａｖａ－ＡＰソフトウェアのインストールが完了する。

【０００５】

【発明が解決しようとする課題】

ところで、移動機内に実現されるＪａｖａ－ＡＰの挙動についての制限は、通信アプリケーションなどの移動機が元から備えているネイティブアプリケーションの挙動についての制限よりも厳しくなっている。例えば、Ｊａｖａ－ＡＰは、移動機内の電話帳データを参照することができないようになっている。このよう

な制限の相違により、悪意をもって作成されたＪａｖａ－ＡＰ、あるいは不具合を有するＪａｖａ－ＡＰによって移動機内の秘密性の高い情報が漏洩したり改竄されたりする事態を確実に回避することができる。

【０００６】

しかし、上述した厳しい制限を全てのＪａｖａ－ＡＰに対して一律に課すだけでは、ユーザやＩＰ（情報提供事業者）の希望を満たすことはできない。例えば、ある程度の信頼性が保証されるのであれば、Ｊａｖａ－ＡＰに移動機に格納された個人情報を参照する権限を与えてもよいと感じるユーザが少なくないと思われる。また、ＩＰにも、移動機に格納されている個人情報や移動機が有する多数の機能の使用を前提としたＪａｖａ－ＡＰを提供したいという希望がある。

【０００７】

これらの希望を満たす仕組みとして、移動機のユーザに対して通信サービスを提供する通信事業者等の信頼できる機関がＪａｖａ－ＡＰに権限を与え、この権限を移動機に通知し、当該権限に基づいて移動機が当該Ｊａｖａ－ＡＰの挙動を制限するという仕組みが考えられる。この仕組みでは、権限の信頼性を保証するために、信頼できる機関以外の他者が権限の付与・管理に関与し得ないようにすべきである。

【０００８】

Ｊａｖａ－ＡＰソフトウェアのダウンロード手順に上述の仕組みを適用する場合、ＡＤＦあるいはＪａｒファイルに権限を示す情報を内包させるのが妥当である。Ｊａｒファイルは ＩＰにより随時更新される種類のファイルであり、ＩＰが保有するのが適当であることから、信頼できる機関に保有させるならＡＤＦが妥当ということになる。

【０００９】

しかし、ＡＤＦはＪａｒファイルに依存した内容となることから、ＩＰが手元のＪａｒファイルを更新されると、信頼できる機関が保有しているＡＤＦの更新も必要になってくる。ＡＤＦは信頼できる機関において他者の他の関与を排するように管理されるのであるから、ＡＤＦの更新作業は繁雑な作業となると予想される。また、Ｊａｒファイルを更新せずとも、ＡＤＦの更新が必要となることが

ある。例えば、ＩＰにおいて、あるＪａｒファイルへのアクセスが集中し、このＪａｒファイルを他のサーバ装置へ移動する場合である。この場合、Ｊａｒファイルの格納位置が変更されるから、ＡＤＦに内包されているパッケージＵＲＬを変更する必要がある。

【００１０】

本発明は、上述した事情に鑑みて為されたものであり、依存関係にある複数のファイルを配信することで配信される、アプリケーションを実現するためのソフトウェアを、ＩＰの自由度を制限することなく、権限に応じた挙動をアプリケーションに対して許可する端末装置へ配信する配信方法および配信システムを提供することを目的としている。

【００１１】

【課題を解決するための手段】

上述した課題を解決するために、本発明は、アプリケーションを実現するためのソフトウェアを内包した実体ファイルを格納した情報提供サーバ装置と、前記実体ファイルに依存した内容を有し前記実体ファイルの格納位置を示すアプリケーション記述ファイルを格納した情報提供サーバ装置と、前記アプリケーション記述ファイルの格納位置を示す第１の識別情報と前記端末装置が前記ソフトウェアを実行することにより実現されるアプリケーションに与えられた権限を示す権限情報とを内包したセキュリティ記述ファイルを格納した管理サーバ装置とを有し、ファイルの格納位置を通知されると当該ファイルを返送する通信システムが、アプリケーションに与えられた権限に応じた挙動を当該アプリケーションに対して許可する端末装置へ前記セキュリティ記述ファイルを、セキュリティを確保して送信する権限送信過程と、前記端末装置が、前記権限送信過程にて前記管理サーバ装置から送信された前記セキュリティ記述ファイルに内包されている前記第１の識別情報を用いて前記アプリケーション記述ファイルを取得する依存情報取得過程と、前記端末装置が、前記依存情報取得過程にて取得した前記アプリケーション記述ファイルを用いて前記通信システムから前記実体ファイルを取得するプログラム取得過程とを有する配信方法を提供する。

【００１２】

この配信方法によれば、端末装置は、アプリケーションに対応したアプリケーション記述ファイルおよび実体ファイルを取得する前に、セキュリティが確保された上で通信システムから送信されるセキュリティ記述ファイルを取得する。このセキュリティ記述ファイルにはアプリケーションに与えられた権限が示されており、端末装置では、取得したセキュリティ記述ファイルに示される権限に応じた挙動が当該セキュリティ記述ファイルに対応するアプリケーションに許可される。

【００１３】

また、本発明は、アプリケーションを実現するためのソフトウェアを内包した実体ファイルを格納した情報提供サーバ装置と、前記実体ファイルに依存した内容を有し前記実体ファイルの格納位置を示すアプリケーション記述ファイルを格納した情報提供サーバ装置と、前記アプリケーション記述ファイルの格納位置を示す第１の識別情報と前記端末装置が前記ソフトウェアを実行することにより実現されるアプリケーションに与えられた権限を示す権限情報とを内包したセキュリティ記述ファイルを格納した管理サーバ装置とを有し、ファイルの格納位置を通知されると当該ファイルを返送する通信システムと、

アプリケーションに与えられた権限に応じた挙動を当該アプリケーションに対して許可する端末装置とを有し、

前記管理サーバ装置は、前記セキュリティ記述ファイルを前記端末装置へ、セキュリティを確保して送信し、前記端末装置は、前記通信システムから送信された前記セキュリティ記述ファイルに内包されている前記第１の識別情報を用いて前記アプリケーション記述ファイルを取得し、前記アプリケーション記述ファイルを用いて前記通信システムから前記実体ファイルを取得する配信システムを提供する。

【００１４】

この配信システムによれば、端末装置は、アプリケーションに対応したアプリケーション記述ファイルおよび実体ファイルを取得する前に、セキュリティが確保された上で通信システムから送信されるセキュリティ記述ファイルを取得することになる。このセキュリティ記述ファイルにはアプリケーションに与えられた

権限が示されており、端末装置では、取得したセキュリティ記述ファイルに示される権限に応じた挙動が当該セキュリティ記述ファイルに対応するアプリケーションに許可される。

【００１５】

【発明の実施の形態】

以下、図面を参照して、本発明の実施の一形態である配信システムについて図面を参照して説明する。なお、図面において、共通する部分には同一の符号が付されている。

この配信システムは、移動通信網を管理する通信事業者（信頼できる機関）が、移動機にインストール可能なＪａｖａ－ＡＰソフトウェアをダウンロードするための情報を移動機のユーザへ提示し、この提示を受けたユーザが、移動機を操作して所望のＪａｖａ－ＡＰソフトウェアを移動機にダウンロードおよびインストールし、移動機において起動するためのものである。なお、本システムにおけるＪａｖａ－ＡＰソフトウェアのダウンロードは、当該Ｊａｖａ－ＡＰソフトウェアの内容を説明した画面を移動機のユーザに提示した後にＡＤＦを配信し更にＪａｒファイルを配信するという手順で行われる。

【００１６】

（１）構成

図１に示されるように、この配信システムは、インターネット１１に接続されたＩＰサーバ装置１２～１４と、通信事業者が移動パケット通信サービスを提供するために用いる移動パケット通信網１５との間で無線パケット通信を行うことが可能であり、移動パケット通信網１５を介して通信相手とパケット通信を行うことができる移動機１６と、インターネット１１と移動パケット通信網１５とを相互接続するゲートウェイサーバ装置１７と、専用線によりゲートウェイサーバ装置１７に接続された管理サーバ装置１８とを有する。このシステムには多数の移動機が存在するが、図面が繁雑になるのを避けるために一つの移動機１６のみが図示されている。これと同様の理由により、３つのＩＰサーバ装置１２～１４のみが図示されている。

【００１７】

（１－１）ＩＰサーバ装置

ＩＰサーバ装置１２は第１のＩＰに管理されており、ＩＰサーバ装置１３および１４は第１のＩＰと異なる第２のＩＰにより管理されている。ＩＰサーバ装置１２～１４はＷＷＷを構成しており、それぞれ一般的なＷＷＷサーバ装置と同様のハードウェアおよび機能を有する。また、ＩＰサーバ装置１２は不揮発性メモリ１２Ａ、ＩＰサーバ装置１３は不揮発性メモリ１３Ａ、ＩＰサーバ装置１４は不揮発性メモリ１４Ａを有し、ＩＰサーバ装置１２～１４はそれぞれ、ＴＣＰに従ったコネクション（以後、ＴＣＰコネクション）を通信相手との間に確立し、このコネクションを介してＨＴＴＰのＧＥＴメソッドを用いた要求メッセージを受信すると、当該ＧＥＴメソッドに指定されたＵＲＬで特定されるファイルを自身の不揮発性メモリから読み出し、このファイルを含むＨＴＴＰの応答メッセージを返送して当該コネクションを切断する。

【００１８】

不揮発性メモリ１２Ａ、１３Ａおよび１４Ａはそれぞれハードディスク等の不揮発性メモリであり、Ｊａｖａプログラミング言語を用いて作成されたプログラムを有するＪａｒファイルと、当該Ｊａｒファイルに関する情報を記述したＡＤＦと、当該プログラムを内包するＪａｖａ－ＡＰソフトウェアの内容を移動機のユーザに説明するための説明ファイルとを記憶し得る。

【００１９】

ＩＰサーバ装置に格納され得るＡＤＦには後述するトラステッドＪａｖａ－ＡＰソフトウェアに対応したＡＤＦと、非トラステッドＪａｖａ－ＡＰソフトウェアに対応したＡＤＦとがある。ＷＷＷにおけるＪａｒファイルの記憶位置を示すパッケージＵＲＬや、Ｊａｒファイルのサイズを示す情報、Ｊａｒファイルの最終変更日時を示す情報等の従来からＡＤＦに記述されている情報は両者にも記述される。これに加えて、トラステッドＪａｖａ－ＡＰソフトウェアに対応したＡＤＦは、図２に示されるように、後述するＡＰＩＤとＪａｒファイルのハッシュ値とを内包し、さらに当該ソフトウェアを提供するＩＰに対してＣＡ（認証局）から付与された秘密鍵で署名される。

【００２０】

また、説明ファイルはＨＴＭＬに従って記述されるテキストファイルであり、移動機においてＨＴＭＬに従って解釈されたときに、このファイルに対応するＪａｖａ－ＡＰソフトウェアをダウンロードするときにユーザにより操作されるオブジェクトと当該Ｊａｖａ－ＡＰソフトウェアに対応するＳＤＦ（セキュリティ記述ファイル。ＳＤＦが存在しない場合にはＡＤＦ）がＷＷＷにおいて記憶されている位置を示すＵＲＬとが対応付けられたＵＩ（ユーザインターフェイス）が提供されるように記述されている。なお、ＳＤＦについては後述する。

また、ＩＰサーバ装置１２～１４の各々は、対応するＩＰの指示に従って上記各ファイルを作成および更新する機能を備えている。

【００２１】

（１－２）ゲートウェイサーバ装置

ゲートウェイサーバ装置１７は前述の通信事業者により管理されており、移動パケット通信網１５とインターネット１１とを接続する一般的なゲートウェイサーバ装置と同様の構成を有し、移動パケット通信網１５とインターネット１１と管理サーバ装置１８との間で相互に通信を中継する。

【００２２】

（１－３）管理サーバ装置

管理サーバ装置１８は前述の通信事業者により管理されており、ＷＷＷを構成し、一般的なＷＷＷサーバ装置と同様のハードウェアおよび機能を有する。また、管理サーバ装置１８はハードディスク等の不揮発性メモリ１８Ａを有し、ＴＣＰコネクションを通信相手との間に確立し、このコネクションを介してＨＴＴＰのＧＥＴメソッドを用いた要求メッセージを受信すると、当該ＧＥＴメソッドに指定されたＵＲＬで特定されるファイルを不揮発性メモリ１８Ａから読み出し、このファイルを含むＨＴＴＰの応答メッセージを返送して当該コネクションを切断する。

【００２３】

また、上記不揮発性メモリ１８Ａには、移動機１６にダウンロード可能なＪａｖａ－ＡＰソフトウェアを移動機１６のユーザに紹介するためのリストファイル２００と、移動機のトラステッドＡＰＩ（APplication Interface）を使用する

ＪａｖａーＡＰを移動機において実現するためのＪａｖａーＡＰソフトウェアを移動機にダウンロードする際に必須のファイルであって、当該ＪａｖａーＡＰソフトウェアについて上記通信事業者と当該ＪａｖａーＡＰソフトウェアを提供するＩＰとの間で結ばれた契約に従って当該通信事業者により作成されるＳＤＦとが記憶される。なお、トラステッドＡＰＩについては後述する。

【００２４】

上記リストファイル２００はＨＴＭＬに従って記述されたテキストファイルであり、ＨＴＭＬに従って解釈された場合に、ＪａｖａーＡＰソフトウェア毎に対応した選択肢と、当該ＪａｖａーＡＰソフトウェアの説明ファイルがＷＷＷにおいて記憶されている位置を示すＵＲＬとが対応付けられたＵＩが提供されるように記述されている。

【００２５】

（１－４）移動機

移動機１６は、図３に示されるように、移動機１６は、ＯＳ（オペレーティングシステム）ソフトウェア、ＪａｖａーＡＰを実行する環境を構築するためのＪａｖａーＡＰ環境ソフトウェア、および各種ネイティブＡＰソフトウェア等を記憶したＲＯＭ１６Ａと、ＲＯＭ１６Ａに接続されＲＯＭ１６Ａからプログラムを読み出して実行するＣＰＵ１６Ｂと、ＣＰＵ１６Ｂに接続された表示部１６Ｃ、不揮発性メモリ１６Ｄ、ＲＡＭ１６Ｅ、通信部１６Ｆおよび操作部１６Ｇを有する。

【００２６】

表示部１６Ｃは例えば液晶表示パネルを有し、ＣＰＵ１６Ｂから供給されるデータで表される画像を表示する。不揮発性メモリ１６Ｄは例えばＳＲＡＭやＥＥＰＲＯＭであり、ＣＰＵ１６Ｂによりデータを読み書きされる。詳しくは後述するが、不揮発性メモリ１６Ｄは、ＷＷＷを構成するサーバ装置（以後、Ｗｅｂサーバ装置）からダウンロードしたＪａｖａーＡＰソフトウェア（ＡＤＦおよびＪａｒを内包する）や、ＳＤＦを記憶するために使用される。

【００２７】

通信部１６Ｆは移動パケット通信網１５と無線パケット通信を行うものであり

、ＣＰＵ１６Ｂと移動パケット通信網１５との間でパケットを中継する。また、通信部１６Ｆは、アンテナや無線送受信部の他に、通話のためのＣＯＤＥＣやマイク、スピーカ等を備えており、移動機１６は図示せぬ移動通信網を介して回線交換による通話を行うこともできる。操作部１６Ｇは操作子を備え、操作子の操作に応じた信号をＣＰＵ１６Ｂへ供給する。

【００２８】

図示せぬ電源が投入されると、ＣＰＵ１６ＢはＲＡＭ１６Ｅをワークエリアとし、ＲＯＭ１６ＡからＯＳソフトウェアに内包されているプログラムを読み出して実行する。これにより、ＣＰＵ１６ＢにはＵＩ等を提供する機能が実現される。すなわち、ＣＰＵ１６ＢはＯＳソフトウェアを起動して移動機１６内にて図４のＯＳを実現する。ＯＳは操作部１６Ｇから供給される信号とＵＩの状態とに基づいてユーザの指示を特定し、この指示に応じた処理を行う。

【００２９】

ユーザの指示がネイティブＡＰソフトウェアである通信ソフトウェアの起動を要求するものであれば、ＯＳは通信ソフトウェアを起動して移動機１６内にて通信ＡＰを実現する。この通信ＡＰを用いることで、ユーザは通話相手と通話をすることができる。

【００３０】

ユーザの指示がネイティブＡＰソフトウェアである電話帳ＡＰの起動を要求するものであれば、ＯＳは電話帳ソフトウェアを起動して移動機１６内にて電話帳ＡＰを実現する。この電話帳ＡＰを用いることで、ユーザは、不揮発性メモリ１６Ｄに記憶された電話帳の内容（以後、電話帳データ）を参照・使用・変更することができる。

【００３１】

ユーザの指示がネイティブＡＰソフトウェアであるＷｅｂブラウザソフトウェアの起動を要求するものであれば、ＯＳはＷｅｂブラウザソフトウェアを起動して移動機１６内にてＷｅｂブラウザを実現する。Ｗｅｂブラウザは ＵＩを提供し、このＵＩの状態と操作部１６Ｇから供給される信号とに基づいてユーザの指示を特定し、この指示に応じた処理を行う。例えば、当該指示が指定されたファイ

ルをWWWから取得する旨の指示の場合には、通信部１６Ｆを制御して当該ファイルを記憶したＷｅｂサーバ装置との間にＴＣＰコネクションを確立し、このコネクションを介して、指定された位置を示すＵＲＬをＧＥＴメソッドに指定したＨＴＴＰの要求メッセージを送信し、この要求メッセージに対応する応答メッセージを受信し、当該コネクションを切断する。さらに、Ｗｅｂブラウザは、受信した応答メッセージに内包されているファイルをＨＴＭＬに従って解釈し、Ｗｅｂページを内包するＵＩを生成し、ユーザに提供する。また、ユーザの指示がＪａｖａ－ＡＰソフトウェアのダウンロードを要求するものである場合には、この指示を次に述べるＪＡＭ（Java Application Manager）に通知する。具体的には、Ｗｅｂページにおいて、オブジェクトタグが指定されているアンカータグで表されるアンカーが押下（クリック操作またはプレス操作）されると、Ｗｅｂブラウザは当該オブジェクトタグのｄａｔａ属性に指定されているＵＲＬを抽出し、当該ＵＲＬからのＪａｖａ－ＡＰソフトウェアのダウンロードが要求されたことをＪＡＭに通知する。

【００３２】

ユーザの指示がネイティブＡＰソフトウェアであるＪＡＭソフトウェアの起動を要求するものであれば、ＯＳはＪＡＭソフトウェアを起動して移動機１６内にてＪＡＭを実現する。ＪＡＭは、移動機１６にインストールされているＪａｖａ－ＡＰソフトウェアの一覧をユーザに提示し、ユーザにより指定されたＪａｖａ－ＡＰソフトウェアを起動する。具体的には、ＪＡＭに対するユーザの指示がＪａｖａ－ＡＰソフトウェアの起動を要求するものであれば、Ｊａｖａ－ＡＰ環境ソフトウェアが起動されて移動機１６内にＪａｖａ－ＡＰ環境が実現され、次に、指定されたＪａｖａ－ＡＰソフトウェアが起動されてＪａｖａ－ＡＰ環境内にＪａｖａ－ＡＰが実現される。Ｊａｖａ－ＡＰ環境は、携帯端末に適した軽量のＪａｖａ仮想マシンであるＫＶＭと、Ｊａｖａ－ＡＰに対して提供されるＡＰＩとを有する。Ｊａｖａ－ＡＰに対して提供されるＡＰＩは、通信事業者がＩＰとの契約に基づいて信頼性を保証したＪａｖａ－ＡＰ（以後、トラステッドＡＰ）のみに使用が許可されるトラステッドＡＰＩと、あらゆるＪａｖａ－ＡＰに使用が許可される非トラステッドＡＰＩとに分けられる。

【００３３】

また、ＪＡＭは、Ｊａｖａ－ＡＰのダウンロードを要求する指示がＷｅｂブラウザから通知されると、Ｊａｖａ－ＡＰソフトウェアを移動機１６にダウンロードしインストールする処理を行う。この処理の流れを図５に示す。

図５に示されるように、ＪＡＭは、まず、ダウンロードしようとするＪａｖａ－ＡＰソフトウェアがトラステッドＡＰを実現するためのＪａｖａ－ＡＰソフトウェア（以後、トラステッドＪａｖａ－ＡＰソフトウェア）であるか否かを判定する（ステップＳ１１）。具体的には、ＪＡＭは、Ｗｅｂブラウザから通知されたＵＲＬの末尾のファイル名を参照し、このファイルの拡張子が“sdf”であればトラステッドＪａｖａ－ＡＰソフトウェア、“sdf”でなければ非トラステッドＪａｖａ－ＡＰソフトウェアであると判定する。ダウンロードしようとするＪａｖａ－ＡＰソフトウェアがトラステッドＪａｖａ－ＡＰソフトウェアであると判定された場合には、従来と同様のダウンロードおよびインストール処理が行われる（ステップＳ１２）。

【００３４】

ダウンロードしようとするＪａｖａ－ＡＰソフトウェアがトラステッドＪａｖａ－ＡＰソフトウェアと判定された場合には、ＪＡＭは、当該ソフトウェアに対応するＳＤＦを管理サーバ装置１８から取得する（ステップＳ１３）。すなわち、ＪＡＭは、管理サーバ装置１８との間にＴＣＰコネクションを確立し、このコネクションを介して、Ｗｅｂブラウザから通知されたＵＲＬで示される位置に記憶されたＳＤＦの送信を管理サーバ装置１８に要求する内容の要求メッセージを生成・送信し、このメッセージに対する応答メッセージを受信し、上記コネクションを切断する。

【００３５】

ＳＤＦは、トラステッドＡＰ毎に通信事業者により作成されるファイルであり、図６に示されるように、トラステッドＪａｖａ－ＡＰソフトウェアを一意に識別するためのＡＰＩＤ、後述するポリシー情報、当該Ｊａｖａ－ＡＰソフトウェアに対応したＡＤＦの記憶位置を示すＵＲＬであるＡＤＦ－ＵＲＬ、および当該Ｊａｖａ－ＡＰソフトウェアを提供するＩＰに対してＣＡが付与した公開鍵を有

する。ＪＡＭは、応答メッセージに内包されているＳＤＦからＡＰＩＤとＡＤＦ－ＵＲＬと公開鍵を抽出するとともに、当該ＳＤＦを不揮発性メモリ１６Ｄに書き込む。

【００３６】

次に、ＪＡＭはＡＤＦを取得する（ステップＳ１４）。具体的には、ＪＡＭは、ＳＤＦから抽出したＡＤＦ－ＵＲＬで特定されるＡＤＦを記憶したＷｅｂサーバ装置との間にＴＣＰコネクションを確立し、当該ＡＤＦの送信を要求する内容の要求メッセージを生成・送信し、このメッセージに対する応答メッセージを受信し、当該ＴＣＰコネクションを切断する。

【００３７】

トラステッドＪａｖａ－ＡＰソフトウェアに対応するＡＤＦは非トラステッドＪａｖａ－ＡＰソフトウェアに対応する通常のＡＤＦとは異なり、前述のＡＰＩＤとＪａｒファイルのハッシュ値とを内包し、さらに当該トラステッドＪａｖａ－ＡＰソフトウェアを提供するＩＰに対してＣＡが付与した秘密鍵により署名（暗号化）されている。ＪＡＭは、応答メッセージに内包されているＡＤＦの署名をＳＤＦから抽出された公開鍵を用いて検証し（復号し）、当該ＡＤＦの正当性を判断する（ステップＳ１５）。

【００３８】

ＡＤＦが正当であると判断した場合には、ＪＡＭは、ＳＤＦから抽出したＡＰＩＤとＡＤＦに内包されているＡＰＩＤとを比較し、両者が一致するか否かを判定する（ステップＳ１６）。両者が一致すると判定された場合には、ＪＡＭは、当該トラステッドＪａｖａ－ＡＰソフトウェアを移動機１６にインストール可能か否かをＡＤＦの内容に基づいて判定する（ステップＳ１７）。この判定の基準は従来と同様である。

【００３９】

インストール可能と判定された場合には、ＪＡＭは、Ｊａｒファイルを取得する。具体的には、ＪＡＭは、当該ＡＤＦを移動機１６に書き込むとともに、当該ＡＤＦからハッシュ値とパッケージＵＲＬを抽出する。さらにＪＡＭは、このパッケージＵＲＬで特定されるＪａｒファイルを記憶したＷｅｂサーバ装置との間

にＴＣＰコネクションを確立し、当該Ｊａｒファイルの送信を要求する内容の要求メッセージを生成・送信し、このメッセージに対する応答メッセージを受信し、当該ＴＣＰコネクションを切断する（ステップＳ１８）。

【００４０】

さらに、ＪＡＭは、取得したＪａｒファイルに対するハッシュ値を算出する（ステップＳ１９）。ハッシュ値の算出に使用するハッシュ関数は任意であるが、移動機で使用されるハッシュ関数とＡＤＦに含まれるハッシュ値の算出時に使用されるハッシュ関数は一致していなければならない。実際には、移動機で使用されるハッシュ関数を用いて、トラステッドＪａｖａ－ＡＰソフトウェアを提供するＩＰがハッシュ値を算出してＡＤＦを生成することになる。

【００４１】

ＪＡＭは、ＪＡＭが算出したハッシュ値とＡＤＦから抽出したハッシュ値とを比較し（ステップＳ２０）、両者が一致した場合には、取得したＪａｒファイルを管理サーバ装置１８に書き込み、トラステッドＪａｖａ－ＡＰソフトウェアのインストールに係る各種処理を行い（ステップＳ２１）、インストールに成功した旨をユーザに通知する（ステップＳ２２）。

【００４２】

なお、ＡＤＦが正当でないと判断した場合、ＳＤＦが有するＡＰＩＤとＡＤＦが有するＡＰＩＤが不一致の場合、インストールしようとするＪａｖａ－ＡＰソフトウェアをインストール可能ではないと判断した場合、算出したハッシュ値とＡＤＦが有するハッシュ値とが不一致の場合には、ＪＡＭは、インストールに失敗した旨をユーザに通知するとともに、移動機１６の状態を、ＳＤＦの取得を開始する前の状態に戻す。

【００４３】

また、ＪＡＭは、Ｊａｖａ－ＡＰの挙動を監視し、トラステッドＡＰＩの使用を制限する。この制限は不揮発性メモリ１６Ｄに記憶されるＳＤＦ内のポリシー情報に従って行われる。ＳＤＦ内のポリシー情報は、例えば図７に概念的に示されるような内容となっている。図７に示されるポリシー情報では、移動機に格納された電話帳データを参照するときに必須のトラステッドＡＰＩである“getPho

neList()”と移動機の状態を取得するときに必須のトラステッドＡＰＩである“getMsStatus()”の使用が許可され、移動機に格納された発着信履歴データを参照するときに必須のトラステッドＡＰＩである“getCallHistory()”の使用が禁止されている。

【００４４】

（２）動作例

次に、上述したシステムの動作例について説明する。

なお、以下に述べる動作において、ＴＣＰコネクションの確立および切断動作についてはＨＴＴＰにおける一般的な動作となることから、それらの説明を省略する。また、前述のＯＳ、Ｗｅｂブラウザ、ＪＡＭ、Ｊａｖａ－ＡＰ、ネイティブＡＰ等が行う動作は移動機１６の動作となることから、以降の説明では、動作の主体を移動機１６とする。

また、図８に示されるように、管理サーバ装置１８の不揮発性メモリ１８Ａには、リストファイル２００とＳＤＦ２０４が記憶されているものとする。これらはＩＰサーバ装置１３およびＩＰサーバ装置１４を管理するＩＰと管理サーバ装置１８を管理する通信事業者との間で結ばれた契約に従って通信事業者により作成されている。これらのうち、リストファイル２００は、移動機１６において解釈・実行されると図９に示されるリストページ２０１を提供するように記述されている。また、リストファイル２００は、リストページ２０１を構成する選択肢２０１Ａが押下されると（クリックまたはプレスされると）、後述の説明ファイル２０２のＵＲＬ（“http://www.main.bbb.co.jp/ghi.html”）をＧＥＴメソッドのパラメータとして含む要求メッセージが生成されるように記述されている。さらに、リストファイル２００は、リストページ２０１を構成する選択肢２０１Ｂが押下されると（クリックまたはプレスされると）、後述の説明ファイル２０７のＵＲＬ（“http://www.ccc:co.jp/jkl.html”）をＧＥＴメソッドのパラメータとして含む要求メッセージが生成されるように記述されている。

【００４５】

また、ＳＤＦ２０４は、ＡＰＩＤとして“0001”、ポリシー情報として図７に示される内容の情報、ＡＤＦ－ＵＲＬとして“http://www.main.bbb.co.jp/view

er.jam”、および公開鍵としてＩＰサーバ装置１３およびＩＰサーバ装置１４を管理するＩＰに対してＣＡが付与した公開鍵を内包している。

【００４６】

また、ＩＰサーバ装置１２の不揮発性メモリ１２Ａには、「詰め将棋」なる名称のＪａｖａ－ＡＰソフトウェア（以後、第１のＪａｖａ－ＡＰソフトウェア）に対応する説明ファイル２１１、ＡＤＦ２１３およびＪａｒファイル２１４が記憶されているものとする。これらはＩＰサーバ装置１２を管理するＩＰによって作成されている。これらのうち、説明ファイル２１１の内容は図１０に示される通りであり、移動機１６において解釈・実行されると図１１に示される説明ページ２１２を提供するように記述されている。また、ＡＤＦ２１３はパッケージＵＲＬとしてＪａｒファイル２１４のＵＲＬ（“http://www.ccc.co.jp/shogi.jar”）を内包している。

【００４７】

また、ＩＰサーバ装置１２の不揮発性メモリ１２Ａには、「星占い」なる名称のＪａｖａ－ＡＰソフトウェア（以後、第２のＪａｖａ－ＡＰソフトウェア）に対応する説明ファイル２０７、ＡＤＦ２０９およびＪａｒファイル２１０が記憶されているものとする。これらはＩＰサーバ装置１２を管理するＩＰによって作成されている。これらのうち、説明ファイル２０７の内容は図１２に示される通りであり、移動機１６において解釈・実行されると図１３に示される説明ページ２０８を提供するように記述されている。また、ＡＤＦ２０９はパッケージＵＲＬとしてＪａｒファイル２１０のＵＲＬ（“http://www.ccc.co.jp/horoscope.jar”）を内包している。

【００４８】

また、ＩＰサーバ装置１３の不揮発性メモリ１３Ａには、「電話帳ビューア」なる名称のＪａｖａ－ＡＰソフトウェア（以後、第３のＪａｖａ－ＡＰソフトウェア）に対応する説明ファイル２０２、ＡＤＦ２０５およびＪａｒファイル２０６が記憶されているものとする。これらはＩＰサーバ装置１３およびＩＰサーバ装置１４を管理するＩＰによって作成されている。これらのうち、説明ファイル２０２の内容は図１４に示される通りであり、移動機１６において解釈・実行さ

れると図１５に示される説明ページ２０３を提供するように記述されている。ＡＤＦ２０５は、ＡＰＩＤとして“0001”、ハッシュ値としてＪａｒファイル２０６のハッシュ値、パッケージＵＲＬとしてＪａｒファイル２０６のＵＲＬ（“http://www.main.bbb.co.jp/viewer.jar”）を内包しており、ＩＰサーバ装置１３およびＩＰサーバ装置１４を管理するＩＰに対してＣＡが付与した秘密鍵を用いて署名されている。

また、移動機１６は第１～第３のＪａｖａ－ＡＰソフトウェアをインストール可能な状態にあるものとする。

【００４９】

（２－１）インストール動作

まず、Ｊａｖａ－ＡＰソフトウェアを移動機１６にインストールする場合の動作例について、Ｊａｖａ－ＡＰソフトウェア毎に説明する。

【００５０】

（２－１－１）第１のＪａｖａ－ＡＰソフトウェア

第１のＪａｖａ－ＡＰソフトウェアのインストール動作は、ユーザが移動機１６を操作し、説明ファイル２１１の取得を試みることから始まる。これにより、移動機１６では、説明ファイル２１１のＵＲＬ（“http://www.ccc.co.jp/mno.html”）をＧＥＴメソッドのパラメータとして含む要求メッセージｔｍ１２が生成される。この要求メッセージｔｍ１２は、図１６に示されるように、移動機１６から送信されＩＰサーバ装置１２により受信される。ＩＰサーバ装置１２では、この要求メッセージｔｍ１２の内容に対応して説明ファイル２１１を内包した応答メッセージｔｍ１３が生成される。この応答メッセージｔｍ１３はＩＰサーバ装置１２から送信され移動機１６により受信される。移動機１６では、ユーザに対して、説明ファイル２１１の内容に応じたＵＩが提供される。この結果、表示部１６Ｃには、例えば図１１に示すような説明ページ２１２が表示される。

【００５１】

この説明ページ２１２を視たユーザが、説明ページ２１２内のアンカー２１２Ａが押下されるよう移動機１６を操作すると、移動機１６では、図１０の説明ファイル２１１に記述されたアンカータグ（“<A”で始まるタグ）のｉｊａｍ属性

に指定されている値がｉｄ属性に指定されているオブジェクトタグ（“<OBJECT”で始まるタグ）が特定され、このオブジェクトタグのｄａｔａ属性に指定されているＵＲＬ（“http://www.ccc.co.jp/shogi.jam”）が抽出され、このＵＲＬで特定されるＡＤＦ２１３の送信を要求する内容の要求メッセージｔｍ１６が生成される。この要求メッセージｔｍ１６は移動機１６から送信されＩＰサーバ装置１２により受信される。ＩＰサーバ装置１２では、この要求メッセージｔｍ１６の内容に対応してＡＤＦ２１３を内包した応答メッセージｔｍ１７が生成される。この応答メッセージｔｍ１７はＩＰサーバ装置１２から送信され移動機１６により受信される。

【００５２】

移動機１６では、ＡＤＦ２１３の内容に基づいて第１のＪａｖａ－ＡＰソフトウェアをインストール可能か否かが判定される。前述のように、移動機１６は第１のＪａｖａ－ＡＰソフトウェアをインストール可能な状態にあるから、移動機１６では第１のＪａｖａ－ＡＰソフトウェアをインストール可能と判定される。

【００５３】

次に、移動機１６では、ＡＤＦ２１３が不揮発性メモリ１６Ｄ１に書き込まれる。また、移動機１６では、ＡＤＦ２１３からパッケージＵＲＬ（“http://www.ccc.co.jp/shogi.jar”）が抽出され、このパッケージＵＲＬで特定されるＪａｒファイル２１４の送信を要求する内容の要求メッセージｔｍ１８が生成される。この要求メッセージｔｍ１８は移動機１６から送信されＩＰサーバ装置１２により受信される。ＩＰサーバ装置１２では、この要求メッセージｔｍ１８の内容に対応してＪａｒファイル２１４を内包した応答メッセージｔｍ１９が生成される。この応答メッセージｔｍ１９はＩＰサーバ装置１２から送信され移動機１６により受信される。移動機１６ではＪａｒファイル２１４が不揮発性メモリ１６Ｄ１に書き込まれ、第１のＪａｖａ－ＡＰソフトウェアのインストールが完了する。

なお、移動機１６において第１のＪａｖａ－ＡＰソフトウェアをインストール可能ではないと判断された場合、移動機１６の状態は、ＡＤＦ２１３の取得を開始する前の状態に戻る。

【００５４】

（２－１－２）第２のＪａｖａ－ＡＰソフトウェア

第２のＪａｖａ－ＡＰソフトウェアのインストール動作は、ユーザが移動機１６を操作し、説明ファイル２０７またはリストファイル２００の取得を試みることから始まる。説明ファイル２０７の取得を試みることから始まる動作はリストファイル２００の取得を試みることから始まる動作のサブセットになっていることから、ここでは、リストファイル２００の取得を試みることから始まる動作のみについて説明する。

【００５５】

図１７に示されるように、移動機１６では、リストファイル２００のＵＲＬ（“http://www.aaa.co.jp/def.html”）をＧＥＴメソッドのパラメータとして含む要求メッセージｔｍ２０が生成される。この要求メッセージｔｍ２０は移動機１６から送信され管理サーバ装置１８により受信される。管理サーバ装置１８では、この要求メッセージｔｍ２０の内容に対応してリストファイル２００を内包した応答メッセージｔｍ２１が生成される。この応答メッセージｔｍ２１は管理サーバ装置１８から送信され移動機１６により受信される。移動機１６では、応答メッセージｔｍ２１の受信を契機として、応答メッセージｔｍ２１内のリストファイル２００がＨＴＭＬに従って解釈され、移動機１６のユーザに対して、リストファイル２００の内容に応じたＵＩが提供される。この結果、移動機１６の表示部１６Ｃには、例えば図９に示すようなリストページ２０１が表示される。

【００５６】

このリストページ２０１を視たユーザが、リストページ２０１内の選択肢２０１Ｂが押下されるように移動機１６を操作すると、移動機１６では、選択肢２０１Ｂに対応付けられているＵＲＬ（“http://www.ccc.co.jp/jkl.html”）をＧＥＴメソッドのパラメータとして含む要求メッセージｔｍ２２が生成される。この要求メッセージｔｍ２２は移動機１６から送信されＩＰサーバ装置１２により受信される。ＩＰサーバ装置１２では、この要求メッセージｔｍ２２の内容に対応して説明ファイル２０７を内包した応答メッセージｔｍ２３が生成される。この応答メッセージｔｍ２３はＩＰサーバ装置１２から送信され移動機１６により

受信される。移動機１６では、ユーザに対して、説明ファイル２０７の内容に応じたＵＩが提供される。この結果、表示部１６Ｃには、例えば図１３に示すような説明ページ２０８が表示される。

【００５７】

この説明ページ２０８を視たユーザが、説明ページ２０８内のアンカー２０８Ａが押下されるよう移動機１６を操作すると、移動機１６では、図１２の説明ファイル２０７に記述されたアンカータグ（“<A”で始まるタグ）のｉｊａｍ属性に指定されている値がｉｄ属性に指定されているオブジェクトタグ（“<OBJECT”で始まるタグ）が特定され、このオブジェクトタグのｄａｔａ属性に指定されているＵＲＬ（“http://www.ccc.co.jp/horoscope.jam”）が抽出され、このＵＲＬで特定されるＡＤＦ２０９の送信を要求する内容の要求メッセージｔｍ２６が生成される。この要求メッセージｔｍ２６は移動機１６から送信されＩＰサーバ装置１２により受信される。ＩＰサーバ装置１２では、この要求メッセージｔｍ２６の内容に対応してＡＤＦ２０９を内包した応答メッセージｔｍ２７が生成される。この応答メッセージｔｍ２７はＩＰサーバ装置１２から送信され移動機１６により受信される。

【００５８】

移動機１６では、ＡＤＦ２０９の内容に基づいて第２のＪａｖａ－ＡＰソフトウェアをインストール可能か否かが判定される。前述のように、移動機１６は第２のＪａｖａ－ＡＰソフトウェアをインストール可能な状態にあるから、移動機１６では第２のＪａｖａ－ＡＰソフトウェアをインストール可能と判定される。

【００５９】

次に、移動機１６では、ＡＤＦ２０９が不揮発性メモリ１６Ｄ１に書き込まれる。また、移動機１６では、ＡＤＦ２０９からパッケージＵＲＬ（“http://www.ccc.co.jp/horoscope.jar”）が抽出され、このパッケージＵＲＬで特定されるＪａｒファイル２１０の送信を要求する内容の要求メッセージｔｍ２８が生成される。この要求メッセージｔｍ２８は移動機１６から送信されＩＰサーバ装置１２により受信される。ＩＰサーバ装置１２では、この要求メッセージｔｍ２８の内容に対応してＪａｒファイル２１０を内包した応答メッセージｔｍ２９が生成

される。この応答メッセージｔｍ２９はＩＰサーバ装置１２から送信され移動機１６により受信される。移動機１６ではＪａｒファイル２１０が不揮発性メモリ１６Ｄ１に書き込まれ、第２のＪａｖａ－ＡＰソフトウェアのインストールが完了する。

なお、移動機１６において、第２のＪａｖａ－ＡＰソフトウェアをインストール可能ではないと判断された場合、移動機１６の状態は、ＡＤＦ２０９の取得を開始する前の状態に戻る。

【００６０】

（２－１－３）第３のＪａｖａ－ＡＰソフトウェア

第３のＪａｖａ－ＡＰソフトウェアのインストール動作は、ユーザが移動機１６を操作し、説明ファイル２０２またはリストファイル２００の取得を試みることから始まる。説明ファイル２０２の取得を試みることから始まる動作はリストファイル２００の取得を試みることから始まる動作のサブセットになっていることから、説明ファイル２０２の取得を試みることから始まる動作についての説明を省略する。

【００６１】

図１８に示されるように、リストファイル２００の取得を試みることから始まる動作において、移動機１６が応答メッセージｔｍ２１を受信し、例えば図９に示すようなリストページ２０１が表示されるまでは図１７に示す動作と同一の動作が行われる。このリストページ２０１を視たユーザが、リストページ２０１内の選択肢２０１Ａが押下されるように移動機１６を操作すると、移動機１６では、選択肢２０１Ａに対応付けられているＵＲＬ（“http://www.main.bbb.co.jp/ghi.html”）をＧＥＴメソッドのパラメータとして含む要求メッセージｔｍ３２が生成される。この要求メッセージｔｍ３２は移動機１６から送信されＩＰサーバ装置１３により受信される。ＩＰサーバ装置１３では、この要求メッセージｔｍ３２の内容に対応して説明ファイル２０２を内包した応答メッセージｔｍ３３が生成される。この応答メッセージｔｍ３３はＩＰサーバ装置１３から送信され移動機１６により受信される。移動機１６では、ユーザに対して、説明ファイル２０２の内容に応じたＵＩが提供される。この結果、表示部１６Ｃには、例えば

図１５に示すような説明ページ２０３が表示される。

【００６２】

この説明ページ２０３を視たユーザが、説明ページ２０３内のアンカー２０３Ａが押下されるよう移動機１６を操作すると、移動機１６では、図１４の説明ファイル２０２に記述されたアンカータグ（“<A”で始まるタグ）のｉｊａｍ属性に指定されている値がｉｄ属性に指定されているオブジェクトタグ（“<OBJECT”で始まるタグ）が特定され、このオブジェクトタグのｄａｔａ属性に指定されているＵＲＬ（“http://www.aaa.co.jp/abc.sdf”）が抽出され、このＵＲＬで特定されるＳＤＦ２０４の送信を要求する内容の要求メッセージｔｍ３４が生成される。この要求メッセージｔｍ３４は移動機１６から送信され管理サーバ装置１８により受信される。管理サーバ装置１８では、この要求メッセージｔｍ３４の内容に対応してＳＤＦ２０４を内包した応答メッセージｔｍ３５が生成される。この応答メッセージｔｍ３５は管理サーバ装置１８から送信され、ゲートウェイサーバ装置１７及び移動パケット通信網１５を介して移動機１６により受信される。管理サーバ装置１８とゲートウェイサーバ装置１７との間の通信路は専用線であり、ゲートウェイサーバ装置１７はセキュリティの確保された移動パケット通信網１５に直接的に接続されていることから、移動機１６に受信されるまでにＳＤＦ２０４が改竄される虞は無い。

【００６３】

移動機１６において、ＳＤＦ２０４は不揮発性メモリ１６Ｄの不揮発性メモリ１６Ｄ１に書き込まれる。また、移動機１６では、ＳＤＦ２０４からＡＰＩＤ（“0001”）とＡＤＦ－ＵＲＬ（“http://www.main.bbb.co.jp/viewer.jam”）と公開鍵が抽出され、このＡＤＦ－ＵＲＬで特定されるＡＤＦ２０５の送信を要求する内容の要求メッセージｔｍ３６が生成される。この要求メッセージｔｍ３６は移動機１６から送信されＩＰサーバ装置１３により受信される。ＩＰサーバ装置１３では、この要求メッセージｔｍ３６の内容に対応してＡＤＦ２０５を内包した応答メッセージｔｍ３７が生成される。この応答メッセージｔｍ３７はＩＰサーバ装置１３から送信され移動機１６により受信される。

【００６４】

移動機１６ではＳＤＦ２０４から抽出された公開鍵を用いてＡＤＦ２０５の正当性が判断される。前述のように、ＳＤＦ２０４に内包されている公開鍵はＡＤＦ２０５への署名の際に用いた秘密鍵と対応していることから、ＩＰサーバ装置１３内あるいはＩＰサーバ装置１３から移動機１６への通信経路においてＡＤＦ２０５が変更されていない限り、ＡＤＦ２０５が正当であると判断される。

【００６５】

ＡＤＦ２０５が正当であると判断されると、移動機１６では、ＳＤＦ２０４から抽出されたＡＰＩＤとＡＤＦ２０５に内包されているＡＰＩＤとが比較される。前述のように、ＩＰサーバ装置１３におけるＡＤＦ２０５にはＳＤＦ２０４内のＡＰＩＤと一致するＡＰＩＤが記述されるように定められていることから、記述ミス等が無い限り、ＳＤＦ２０４から抽出されたＡＰＩＤとＡＤＦ２０５に内包されているＡＰＩＤは一致する。

【００６６】

ＡＰＩＤが一致すると、移動機１６では、ＡＤＦ２０５の内容に基づいて第３のＪａｖａ－ＡＰソフトウェアをインストール可能か否かが判定される。前述のように、移動機１６は第３のＪａｖａ－ＡＰソフトウェアをインストール可能な状態にあるから、移動機１６では第３のＪａｖａ－ＡＰソフトウェアをインストール可能と判定される。

【００６７】

次に、移動機１６では、ＡＤＦ２０５が不揮発性メモリ１６Ｄ１に書き込まれる。また、移動機１６では、ＡＤＦ２０５からハッシュ値とパッケージＵＲＬ（“http://www.main.bbb.co.jp/viewer.jar”）が抽出され、このパッケージＵＲＬで特定されるＪａｒファイル２０６の送信を要求する内容の要求メッセージｔｍ３８が生成される。この要求メッセージｔｍ３８は移動機１６から送信されＩＰサーバ装置１３により受信される。ＩＰサーバ装置１３では、この要求メッセージｔｍ３８の内容に対応してＪａｒファイル２０６を内包した応答メッセージｔｍ３９が生成される。この応答メッセージｔｍ３９はＩＰサーバ装置１３から送信され移動機１６により受信される。

【００６８】

移動機１６ではＪａｒファイル２０６と所定のハッシュ関数とを用いてハッシュ値が算出され、このハッシュ値とＡＤＦ２０５から抽出されたハッシュ値とが比較される。前述のように、ＡＤＦ２０５には当該ＡＤＦ２０５に対応するＪａｒファイルのハッシュ値が記述されるように定められていることから、記述ミス等がない限り、両ハッシュ値は一致する。両ハッシュ値が一致すると、移動機１６では、Ｊａｒファイル２０６が不揮発性メモリ１６Ｄ１に書き込まれ、第３のＪａｖａ－ＡＰソフトウェアのインストールが完了する。

【００６９】

なお、移動機１６においてＡＤＦ２０５が正当でないと判断された場合や、ＳＤＦ２０４から抽出されたＡＰＩＤとＡＤＦ２０５に内包されているＡＰＩＤが不一致の場合、第３のＪａｖａ－ＡＰソフトウェアをインストール可能ではないと判断された場合、算出したハッシュ値とＡＤＦ２０５から抽出されたハッシュ値とが不一致の場合には、移動機１６の状態は、ＳＤＦ２０４の取得を開始する前の状態に戻る。

【００７０】

（２－２）Ｊａｖａ－ＡＰソフトウェアが起動されている時の移動機１６の挙動

次に、Ｊａｖａ－ＡＰソフトウェアが起動されている時の移動機１６の挙動について説明する。

（２－２－１）第１のＪａｖａ－ＡＰソフトウェア

上述したインストール動作により移動機１６にインストールされた第１のＪａｖａ－ＡＰソフトウェアが、ＪＡＭが実現された移動機１６において起動され、当該ソフトウェアに対応した機能（以後、第１のＪａｖａ－ＡＰ）が移動機１６内に実現されたときの移動機１６の挙動について説明する。

【００７１】

第１のＪａｖａ－ＡＰが使用しようとするＡＰＩが非トラステッドＡＰＩの場合、当該ＡＰＩの使用はＪＡＭにより許可される。したがって、第１のＪａｖａ－ＡＰは当該ＡＰＩを使用することができる。

また、第１のＪａｖａ－ＡＰが使用しようとするＡＰＩがトラステッドＡＰＩの場合、ＪＡＭは当該Ｊａｖａ－ＡＰに対応するＳＤＦが不揮発性メモリ１６Ｄ

に記憶されているか否かを調べる。そのようなＳＤＦは不揮発性メモリ１６Ｄに記憶されていないから、ＪＡＭは第１のＪａｖａ－ＡＰによる当該ＡＰＩの使用を禁止する。したがって、第１のＪａｖａ－ＡＰは当該ＡＰＩの使用することができない。

【００７２】

（２－２－２）第２のＪａｖａ－ＡＰソフトウェア

移動機１６にインストールされた第２のＪａｖａ－ＡＰソフトウェアが、ＪＡＭが実現された移動機１６において起動され、当該ソフトウェアに対応した機能が移動機１６内に実現されたときの移動機１６の挙動は、第１のＪａｖａ－ＡＰソフトウェアが起動されている時の移動機１６の挙動と同様となる。

【００７３】

（２－２－３）第３のＪａｖａ－ＡＰソフトウェア

移動機１６にインストールされた第３のＪａｖａ－ＡＰソフトウェアが、ＪＡＭが実現された移動機１６において起動され、当該ソフトウェアに対応した機能（以後、第３のＪａｖａ－ＡＰ）が移動機１６内に実現されたときの移動機１６の挙動について説明する。

【００７４】

第３のＪａｖａ－ＡＰが使用しようとするＡＰＩが非トラステッドＡＰＩの場合当該ＡＰＩの使用はＪＡＭにより許可される。したがって、第３のＪａｖａ－ＡＰは当該ＡＰＩを使用することができる。

第３のＪａｖａ－ＡＰが使用しようとするＡＰＩがトラステッドＡＰＩの場合、移動機１６の挙動は使用するＡＰＩに依存する。以下、使用するＡＰＩ毎に移動機１６の挙動を説明する。

【００７５】

（２－２－３－１）getPhoneList()

“getPhoneList()”はトラステッドＡＰＩであるから、当該ＡＰＩの使用の可否は、不揮発性メモリ１６Ｄに記憶されているＳＤＦ２０４内のポリシー情報に基づいてＪＡＭにより決定される。このポリシー情報の内容は図７に示される通りであることから、“getPhoneList()”の使用がＪＡＭにより許可される。した

がって、第３のＪａｖａ－ＡＰは“getPhoneList()”を使用することができる。つまり、第３のＪａｖａ－ＡＰは電話帳データを読み出すことができる。

【００７６】

（２－２－３－２）getCallHistory()

“getCallHistory()”はトラステッドＡＰＩであるから、当該ＡＰＩの使用の可否はＳＤＦ２０４内のポリシー情報に基づいてＪＡＭにより決定される。このポリシー情報の内容は図７に示される通りであることから、“getCallHistory()”の使用がＪＡＭにより禁止される。したがって、第３のＪａｖａ－ＡＰは“getCallHistory()”を使用することができない。つまり、第３のＪａｖａ－ＡＰは発着信履歴データを読み出すことができない。

【００７７】

（２－３）第３のＪａｖａ－ＡＰソフトウェアの変更後の動作

次に、ＩＰサーバ装置１３およびＩＰサーバ装置１４を管理するＩＰが第３のＪａｖａ－ＡＰソフトウェアの配信形態や内容を変更した場合の本システム動作について説明する。ただし、ここでの変更は、第３のＪａｖａ－ＡＰソフトウェアの改善等を目的としたＪａｒファイル２０６の内容の変更と、ＩＰサーバ装置１３の負荷の軽減等を目的とした配信形態の変更とを含む。後者の変更を達成するために、ＩＰサーバ装置１３およびＩＰサーバ装置１４を管理するＩＰは、図１９に示すように、変更後のＪａｒファイル２０６（以後、Ｊａｒファイル２１５）をＩＰサーバ装置１４の不揮発性メモリ１４Ａに記憶させ、このＪａｒファイル２１５に対応するようにＡＤＦ２０５の内容を変更してＡＤＦ２１６としている。変更後の第３のＪａｖａ－ＡＰソフトウェアの配信に必要な作業は以上の通りであり、管理サーバ装置１８を管理する通信事業者が行うべき作業は存在しない。

【００７８】

このような変更の後の第３のＪａｖａ－ＡＰソフトウェアのインストール動作は、図２０に示す通りとなる。この図に示す動作が図１８に示す動作と相違し始めるのは、ＩＰサーバ装置１３において、ＡＤＦ２０５を内包した応答メッセージｔｍ３７ではなく、ＡＤＦ２１６を内包した応答メッセージｔｍ４７を生成し

てからである。なお、両図において、応答メッセージｔｍ４７は応答メッセージｔｍ３７、要求メッセージｔｍ４８は要求メッセージｔｍ３８、応答メッセージｔｍ４９は応答メッセージｔｍ３９に対応している。

【００７９】

ＩＰサーバ装置１３において応答メッセージｔｍ４７を生成して以降の動作が、図１８に示す動作と本質的に異なるのは、ＡＤＦ２１６およびＪａｒファイル２１５が処理の対象となる点と、ＡＤＦ２１６に内包されているパッケージＵＲＬ（“http://www.sub.bbb.co.jp/viewer.jar”）で特定されるＪａｒファイル２１５の送信を要求する内容の要求メッセージｔｍ４８が移動機１６にて生成される点と、この要求メッセージｔｍ４８が移動機１６から送信されＩＰサーバ装置１４により受信される点と、ＩＰサーバ装置１４においてＪａｒファイル２１５を内包した応答メッセージｔｍ４９が生成される点と、この応答メッセージｔｍ４９がＩＰサーバ装置１４から送信され移動機１６により受信される点のみである。

【００８０】

（３）変形例

上述した配信システムでは、移動機は、秘密鍵による署名データと公開鍵とを用いてＳＤＦとＡＤＦの作成者との対応関係の正当性を確認するようにしたが、システムに要求されるセキュリティレベルによっては、ＳＤＦに公開鍵を内包させず、ＩＰサーバ装置においてはＡＤＦに対する秘密鍵を用いた署名を行わず、かつ移動機においては当該確認処理を省略する、という形態とし、移動機およびＩＰサーバ装置における処理量や、移動機と管理サーバ装置およびＩＰサーバ装置との間の通信量を低減するようにしてもよい。

【００８１】

また、上述した配信システムでは、Ｊａｒファイルのハッシュ値を当該Ｊａｒファイルに対応するＡＤＦに内包させる一方、移動機において生成し、両者を比較し、ＪａｒファイルとＡＤＦとの対応関係の正当性を確認するようにしたが、システムに要求されるセキュリティレベルによっては、ＡＤＦにハッシュ値を内包させずに当該確認処理を省略する形態とし、移動機およびＩＰサーバ装置にお

ける処理量や移動機とＩＰサーバ装置との間の通信量を低減するようにしてもよい。

【００８２】

また、上述した配信システムでは、トラステッドＪａｖａ－ＡＰに固有のＡＰＩＤを使用してＳＤＦとＡＤＦ（およびＪａｒファイル）との対応が正当であるか否かを判定するようにしたが、トラステッドＪａｖａ－ＡＰを提供する情報提供事業者に固有のＣＩＤを用いてＳＤＦとＡＤＦ（およびＪａｒファイル）との対応が正当であるか否かを判定するようにしてもよい。また、システムに要求されるセキュリティレベルによっては、ＡＰＩＤやＣＩＤを用いた判定を省略するようにしてもよい。

【００８３】

また、上述した配信システムではドメインネームを用いてサーバを指定するようにしたが、ＩＰアドレスを用いてサーバを指定するようにしてもよい。

また、移動機において、ＳＤＦの送信元のサーバ装置のドメインネームを予め設定された文字列と比較し、信頼できる機関が管理するサーバ装置のドメインネームである場合にのみ、ＳＤＦを正当と認める態様としてもよい。この態様では、比較対象の文字列（例えば、通信事業者のドメインネームを示す文字列）は移動機のＲＯＭまたは不揮発性メモリに予め格納されることになる。ＲＯＭに予め格納する態様では、文字列の書き換えが不可能であるから、より高いセキュリティを確保できる。また、不揮発性メモリに予め格納する態様では、移動機の売買後に信頼できる機関を格納することができるので、ユーザおよび信頼できる機関に対して優れた利便性を提供することができる。

【００８４】

また、上述した配信システムでは、ＳＤＦの配信に使用する通信路を提供する通信事業者を信頼できる機関として高いセキュリティを確保するようにしたが、本発明は通信路の提供が信頼できる機関により為されていない態様をも技術的範囲に含む。例えば、信頼できる機関と移動機とを暗号化通信路により接続し、この通信路を介して信頼できる機関がＳＤＦを配信するようにしてもよい。また、通信路のセキュリティが確保されていなくても、ＳＤＦを暗号化した後に配信し

、移動機においてＳＤＦを復号するようにすれば、ある程度のセキュリティを確保してＳＤＦを配信することができる。

【００８５】

上述した配信システムでは、ＨＴＴＰに従ってファイルを送受するようにしたが、ＨＴＴＰＳを使用し、より高いセキュリティを確保するようにシステムを変形してもよい。

また、上述した配信システムにおいて、信頼できる機関がＩＰとなってよいこと、すなわち、管理サーバ装置がＩＰサーバ装置を兼ねるようにしてもよいことは言うまでもない。

【００８６】

さらに、上述した配信システムでは、Ｊａｖａ－ＡＰによる利用を制限する対象としてＡＰＩを挙げたが、本発明はこれに限定されるものではなく、任意の資源（リソース）を対象とすることができる。ここでいう資源はハードウェア資源であってもよいし、後述するネットワーク資源やソフトウェア資源であってもよい。ハードウェア資源としては、メモリやスピーカ、マイク、赤外線コントローラ、ＬＥＤ（Light Emitting Diode）等の移動機が備え得るものや移動機と共働し得るＵＩＭ（User Identity Module）やＳＩＭ（Subscriber Identity Module）等の外部機器なども挙げられる。

【００８７】

次にネットワーク資源について説明する。前述したように、移動機は移動通信網との間で無線通信を行う。この無線通信時には、移動機は、移動通信網により提供される無線チャネル等の無線資源を使用する。この無線資源はネットワーク資源の一種である。また、移動機は無線資源が属する通信プロトコルレイヤよりも高位の通信プロトコルレイヤにおいて、パケットの伝送路や回線接続の通信路などの通信資源を使用する。このような通信資源もネットワーク資源の一種である。

【００８８】

次にソフトウェア資源について説明する。ソフトウェア資源としては、ＡＰＩやクラス、パッケージ等が挙げられる。ソフトウェア資源が提供する機能は様々

であるが、典型的な機能として、暗号演算などの演算処理機能や、Ｗｅｂブラウザ等の他のアプリケーションとの間でデータを送受したりする機能などが挙げられる。また、本発明は、上記外部機器が有するソフトウェア資源をも利用の制限対象とする態様を技術的範囲に含む。

【００８９】

ところで、Ｊａｖａ－ＡＰによるハードウェア資源やネットワーク資源の利用は、ソフトウェア資源を利用して行われるのが一般的である。上述した配信システムにおける移動機も、ハードウェア資源やネットワーク資源を利用するためのソフトウェア資源を有しており、このようなソフトウェア資源の利用を制限することにより、間接的に、ハードウェア資源やネットワーク資源の利用を制限している。このように、間接的な制限の形態としたことにより、多様なソフトウェア資源を用意すれば、Ｊａｖａ－ＡＰのうちのトラステッドＪａｖａ－ＡＰについてのみ、自他のＪａｖａ－ＡＰの権限を変更する権限を与える、またはダウンロード元のサーバ装置としか通信することができないという制限を外す、あるいはメモリの特定の記憶領域に対してアクセスできるようにするといった、複数の資源の制限を細かく変更しなければ実現できないようなことまで容易に指定できるようになる。なお、移動機内部のソフトウェア資源の利用を制限して上記外部機器のソフトウェア資源の利用を間接的に制限する態様も本発明の技術的範囲に含まれる。

【００９０】

なお、パーミッションの表現方法としては、一つの資源と一つのフラグ（許可／禁止）とを対応付けるようにしてもよいし、複数の資源のパーミッションを一つの情報で示すようにしてもよい。

【００９１】

また、本発明では、複数の利用の種類を持つ資源について、利用を許可（あるいは禁止）する種類を示すようにパーミッションを設定することも可能である。この場合、移動機において、より木目細かな制御が実現される。例えば、メモリには読み出しと書き込みの２つの利用形態（利用の種類）があるから、非トラステッドＪａｖａ－ＡＰには読み出しでしか利用されないが、トラステッドＪａｖ

ａ－ＡＰには読み出し及び書き込みの両方で利用され得るようにすることもできる。また、例えば、１つのパケット伝送路を複数のアプリケーションが共用可能な移動機において、パケット伝送路を利用する権限を有するＪａｖａ－ＡＰが起動されている間にＷｅｂブラウザ等が起動された場合、当該Ｊａｖａ－ＡＰが「パケット伝送路の利用を排他的に行う」ことを許可されていないＪａｖａ－ＡＰであればＷｅｂブラウザ等によるパケット伝送路の共用を排除することはできないが、「パケット伝送路の利用を排他的に行う」ことを許可されているＪａｖａ－ＡＰであればパケット伝送路を占有して使用することができる、といった制御が可能となる。さらに、この例を変形することで、ある種のパーミッションを与えられたＪａｖａ－ＡＰはユーザに許可を求めることなくパケット通信路を排他的に利用することが可能であり、別のパーミッションを与えられたＪａｖａ－ＡＰはユーザに許可を求めることなくパケット通信路を利用することが可能だがパケット通信路を排他的に利用するためにはユーザの許可を得ることが必要であり、さらに別のパーミッションを与えられたＪａｖａ－ＡＰはユーザに許可を求めることなくパケット通信路を利用することが可能だがパケット通信路を排他的に利用することは不可能であり、さらに別のパーミッションを与えられたＪａｖａ－ＡＰはユーザの許可を得て初めてパケット通信路を利用することが可能であり、さらに別のパーミッションを与えられたＪａｖａ－ＡＰはパケット通信路を利用することすらできない、といった制御も可能となる。この例から明らかなように、本発明における「利用の種類」には、資源を利用する際に経る手順の種類（ユーザの許可を得る手順／ユーザの許可を得ない手順）も含まれる。

【００９２】

また、上述した配信システムでは全ての移動機に対して同一のリストページが提供されるが、移動機毎に異なるリストページを提供するようにしてもよい。

【００９３】

また、上述の配信システムでは、Ｊａｖａ－ＡＰの実行時にＪａｖａ－ＡＰの挙動を制限するようにしたが、ＩＰサーバ装置に格納されているＪａｒファイルにポリシー情報を内包させ、Ｊａｒファイルのダウンロード時に、移動機において、このポリシー情報とＳＤＦ中とのポリシー情報とを比較し、両者が一致しな

い場合には、当該Ｊａｒファイルに対応するＪａｖａ－ＡＰを起動できないように、あるいは当該Ｊａｒファイルを含むＪａｖａ－ＡＰソフトウェアをインストールできないようにしてもよい。もちろん、両ポリシー情報の一致する項目についてのパーミッションのみを有効とするようにしてもよい。

【００９４】

また、通信事業者がＣＡにより付与された自身の秘密鍵を用いてＳＤＦに署名してからＳＤＦを配信し、移動機においてＣＡが通信事業者に付与した公開鍵を用いてＳＤＦの署名を検証するようにしてもよい。もちろん、通信事業者の公開鍵は予め移動機に格納されていなければならない。公開鍵は予め移動機に格納する方法としては、通信により配信し不揮発性メモリに書き込んでおく方法、ＲＯＭに書き込んだ後に移動機を販売する方法などが考えられる。

また、上述の配信システムではソフトウェアは移動機へ配信されるが、本発明の技術的範囲には、移動機以外の端末装置へ配信する態様も含まれる。

【００９５】

【発明の効果】

以上説明したように、本発明によれば、端末装置では、取得したセキュリティ記述ファイルに示される権限に応じた挙動が当該セキュリティ記述ファイルに対応するアプリケーションに許可される。したがって、多様なアプリケーションを提供することができる。さらに、権限を示す情報は管理サーバ装置からセキュリティが確保された上で端末装置へ送信されるから、権限が第三者により改竄される虞もない。また、依存関係を有するアプリケーション記述ファイルおよび実体ファイルを管理サーバ装置に格納する必要はないことから、ＩＰの自由度が制限されることもない。

【図面の簡単な説明】

【図１】　本発明の実施の一形態に係る配信システムの構成を示すブロック図である。

【図２】　同システムに特有のＡＤＦのデータ構成を示す概念図である。

【図３】　同システムを構成する移動機１６の構成を示すブロック図である。

【図４】　同移動機１６の機能構成を示す概念図である。

【図５】　同移動機１６がＪａｖａ－ＡＰソフトウェアをダウンロードしインストールする処理の流れを示すフローチャートである。

【図６】　同システムにおいて管理サーバ装置１８に格納されているＳＤＦのデータ構成を示す概念図である。

【図７】　同ＳＤＦに内包されるポリシー情報の内容を示す概念図である。

【図８】　同配信システムの動作を説明するためのブロック図である。

【図９】　同配信システムにて配信されるリストページを示す図である。

【図１０】　同配信システムを構成するＩＰサーバ装置１２が格納している説明ファイルの内容を示す図である。

【図１１】　同配信システムにて配信される説明ページを示す図である。

【図１２】　同ＩＰサーバ装置１２が格納している説明ファイルの内容を示す図である。

【図１３】　同配信システムにて配信される説明ページを示す図である。

【図１４】　同配信システムを構成するＩＰサーバ装置１３が格納している説明ファイルの内容を示す図である。

【図１５】　同配信システムにて配信される説明ページを示す図である。

【図１６】　同配信システムの動作を説明するためのシーケンス図である。

【図１７】　同配信システムの動作を説明するためのシーケンス図である。

【図１８】　同配信システムの動作を説明するためのシーケンス図である。

【図１９】　同配信システムの他の動作を説明するためのブロック図である。

【図２０】　同配信システムの他の動作を説明するためのシーケンス図である。

【符号の説明】

１１	インターネット
１２、１３、１４	ＩＰサーバ装置
１５	移動パケット通信網
１６	移動機

１７　　ゲートウェイサーバ装置

１８　　管理サーバ装置

１６Ｄ、１２Ａ、１３Ａ、１４Ａ、１８Ａ　不揮発性メモリ

１６Ａ　　ＲＯＭ

１６Ｂ　　ＣＰＵ

１６Ｃ　　表示部

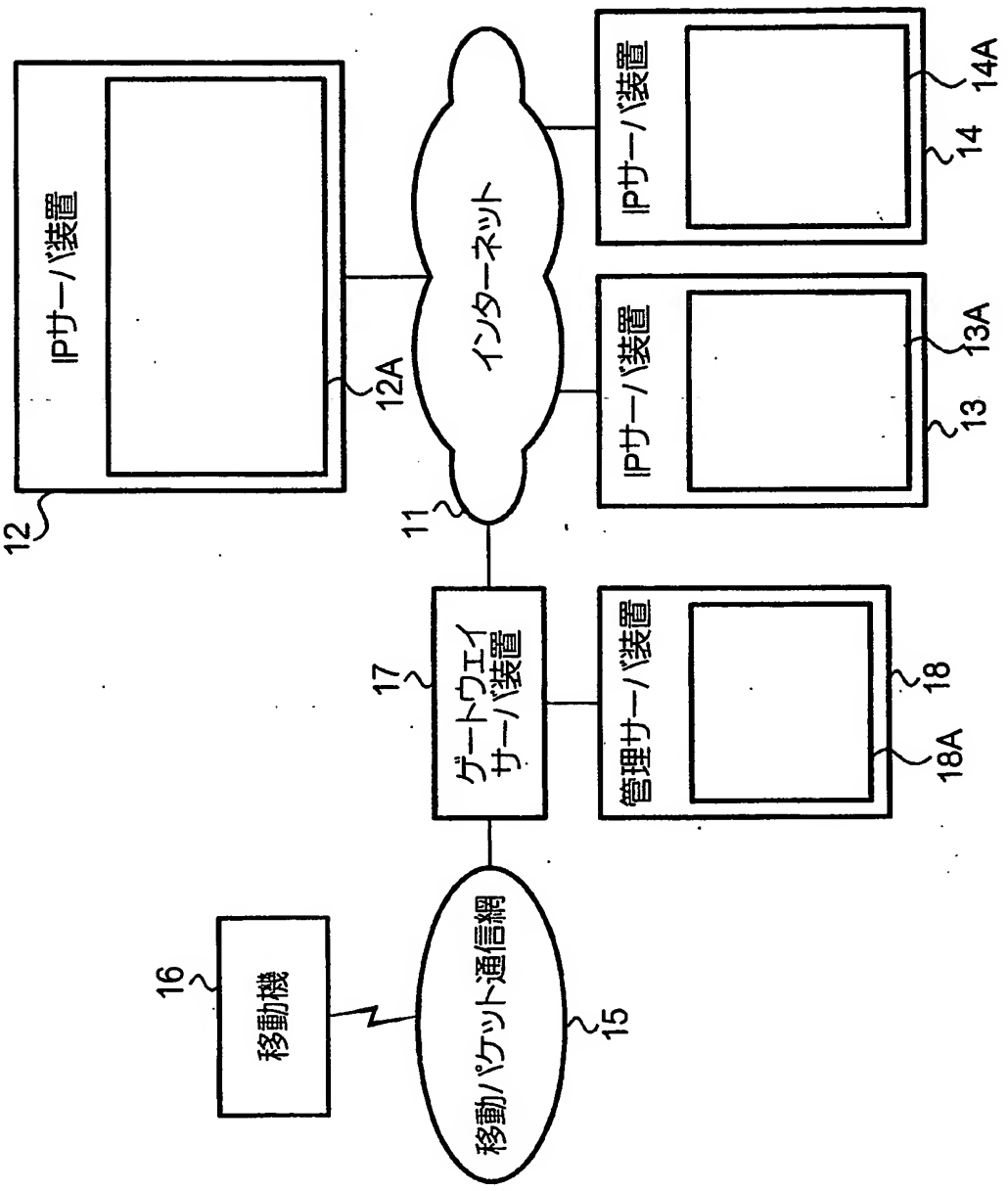
１６Ｅ　　ＲＡＭ

１６Ｆ　　通信部

１６Ｇ　　操作部

【書類名】　　図面

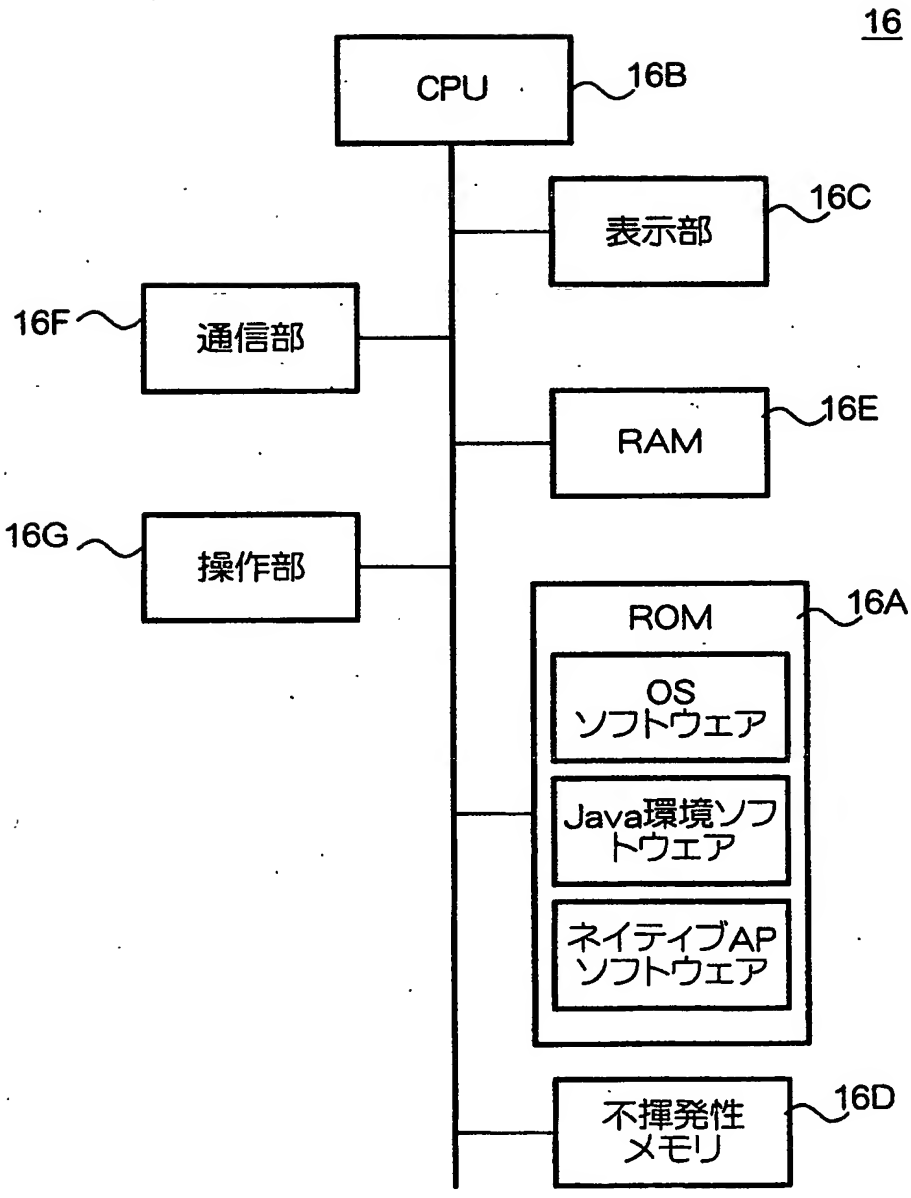
【図１】


IPサーバ装置
12
12A
インターネット
11
IPサーバ装置
14
14A
IPサーバ装置
13
13A
ゲートウエイサーバ装置
17
管理サーバ装置
18
18A
移動パケット通信網
15
移動機
16

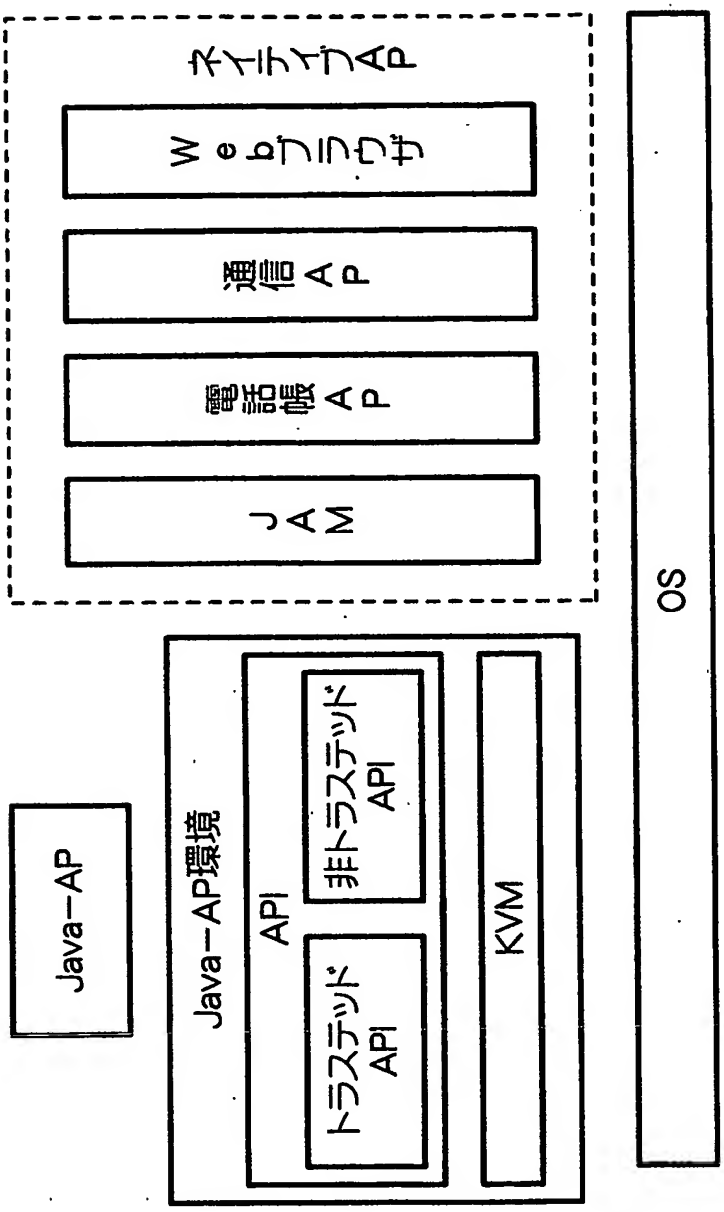
【図２】


APID
ハッシュ値
・・・
パッケージURL

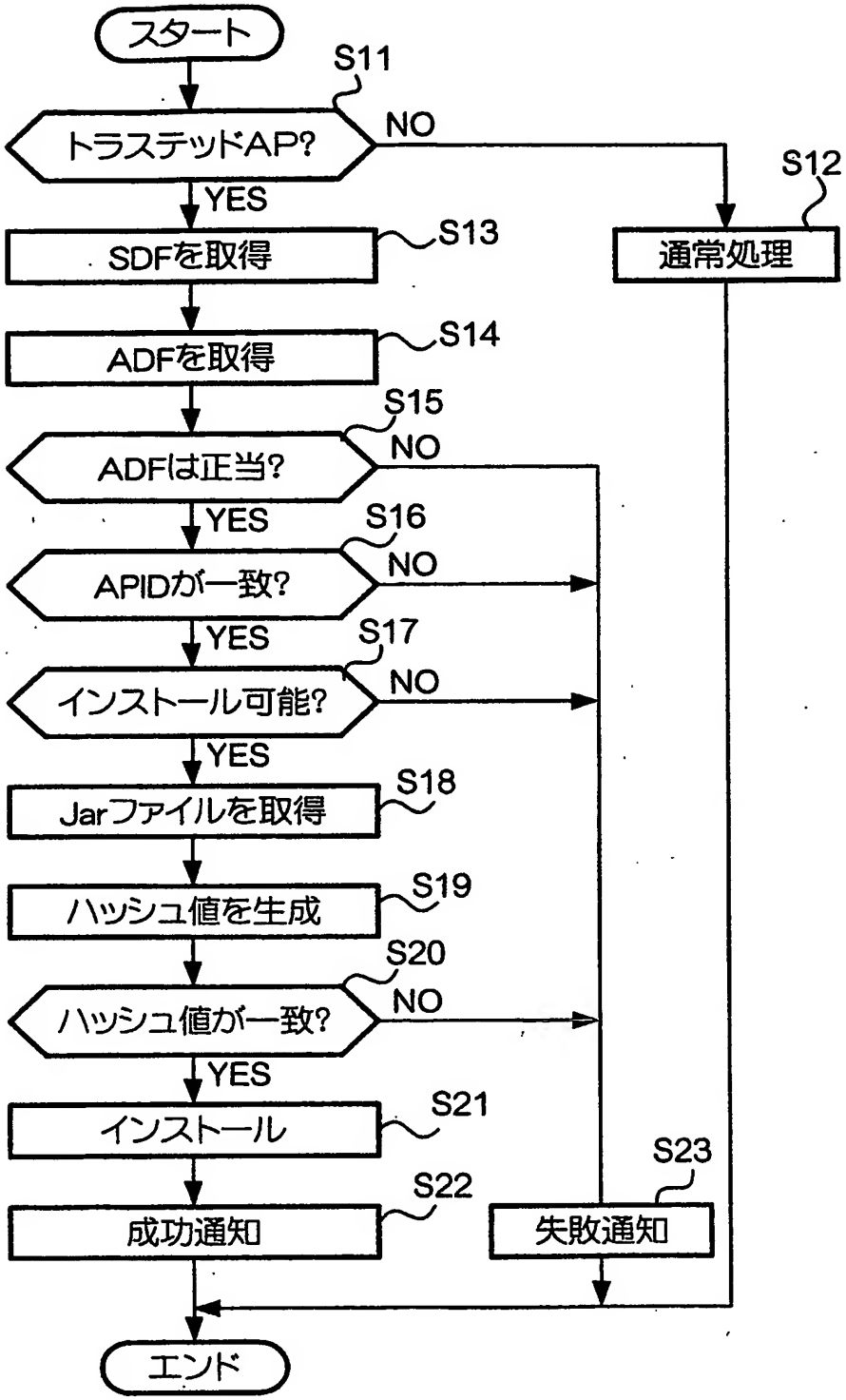
【図３】


16
CPU
16B
表示部
16C
16F
通信部
RAM
16E
16G
操作部
ROM
16A
OS
ソフトウェア
Java環境ソフ
トウェア
ネイティブAP
ソフトウェア
不揮発性
メモリ
16D

【図４】


ネイティブAP
Webブラウザ
通信AP
電話帳AP
JAM
OS
Java−AP環境
API
非トラステッドAPI
トラステッドAPI
KVM
Java−AP

【図５】


スタート
S11
トラステッドAP?
NO
S12
YES
SDFを取得
S13
通常処理
ADFを取得
S14
S15
ADFは正当?
NO
YES
S16
APIDが一致?
NO
YES
S17
インストール可能?
NO
YES
Jarファイルを取得
S18
ハッシュ値を生成
S19
S20
ハッシュ値が一致?
NO
YES
インストール
S21
S23
S22
成功通知
失敗通知
エンド

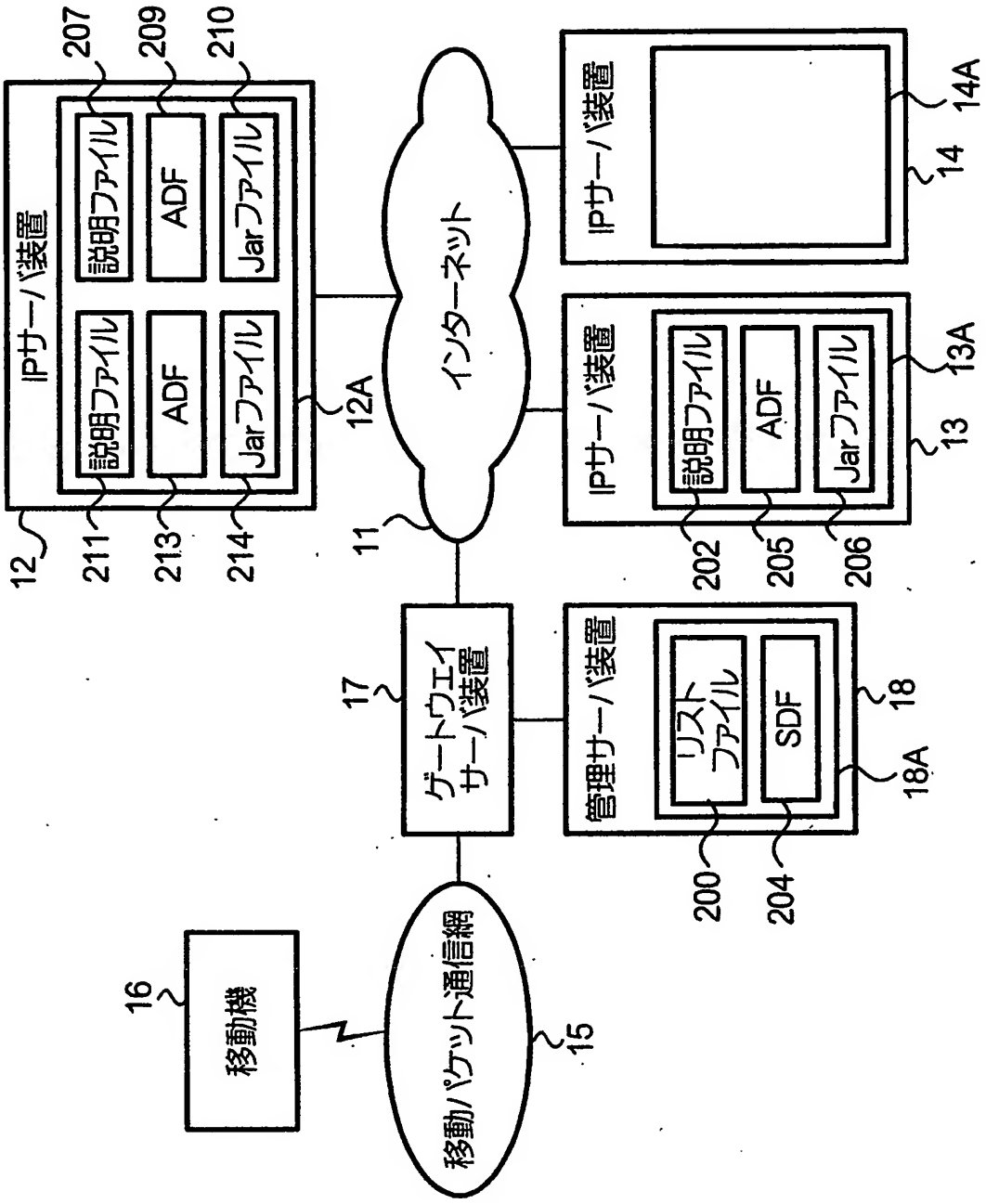
【図６】

APID	ポリシー情報	ADF－URL	公開鍵

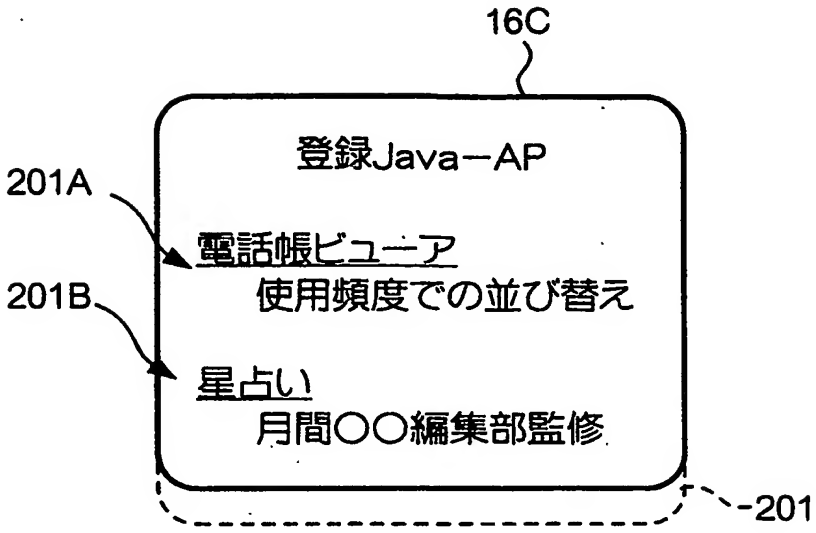
【図７】

トラステッドAPI	パーミッション
getPhoneList()	○
getCallHistory()	×
getMsStatus()	○

【図８】


IPサーバ装置
説明ファイル
ADF
Jarファイル
207
209
210
211
213
214
12
12A
インターネット
11
IPサーバ装置
14
14A
IPサーバ装置
13
13A
202
205
206
ゲートウェイ
サーバ装置
17
管理サーバ装置
リスト
ファイル
SDF
18
18A
200
204
移動パケット通信網
15
移動機
16

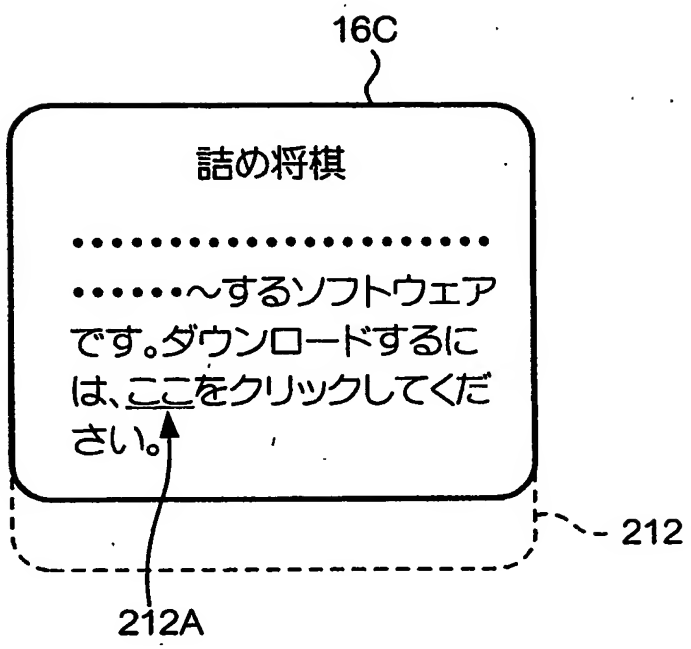
【図９】



【図１０】

```
<OBJECT declare id="application.declaration"
data="http://www.ccc.co.jp/horoscope.jam>
詰め将棋
</OBJECT>
  ～するソフトウェアです。ダウンロードするには
<A ijam="#application.declaration">ここ</A>
をクリック。
```

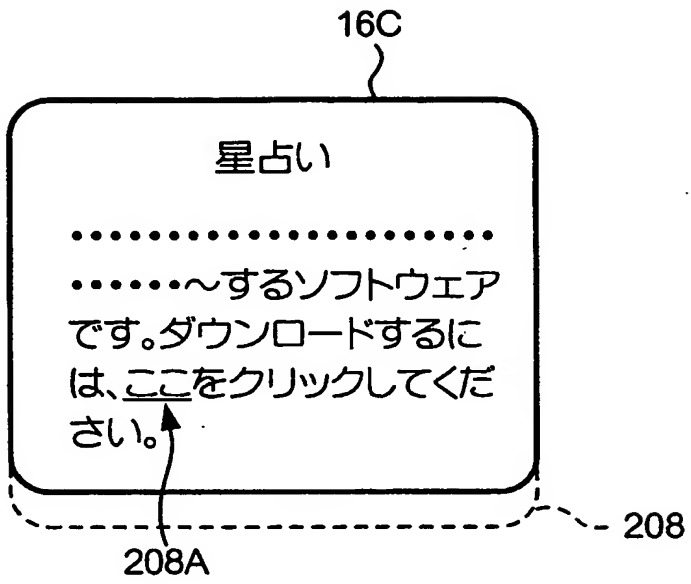
【図１１】



【図１２】

```
<OBJECT declare id="application.declaration"
data="http://www.ccc.co.jp/viewer.jam>
星占い
</OBJECT>
   ～するソフトウェアです。ダウンロードするには
<A ijam="#application.declaration">ここ</A>
をクリック。
```

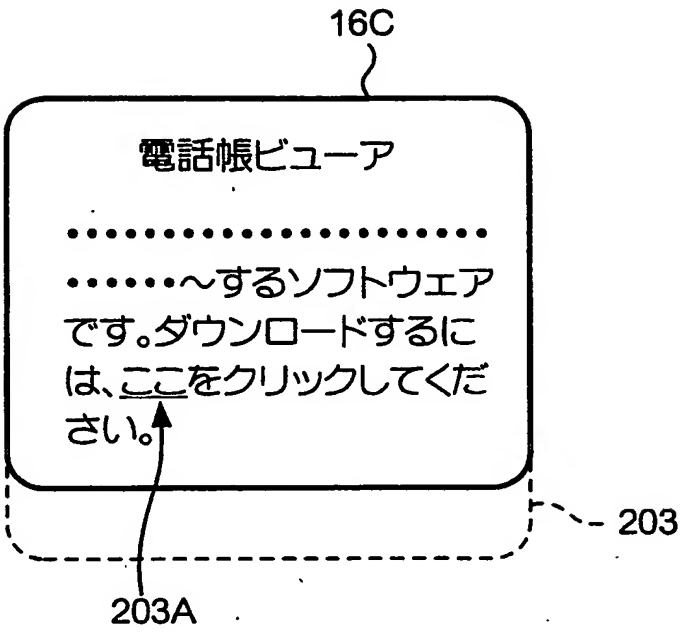
【図１３】



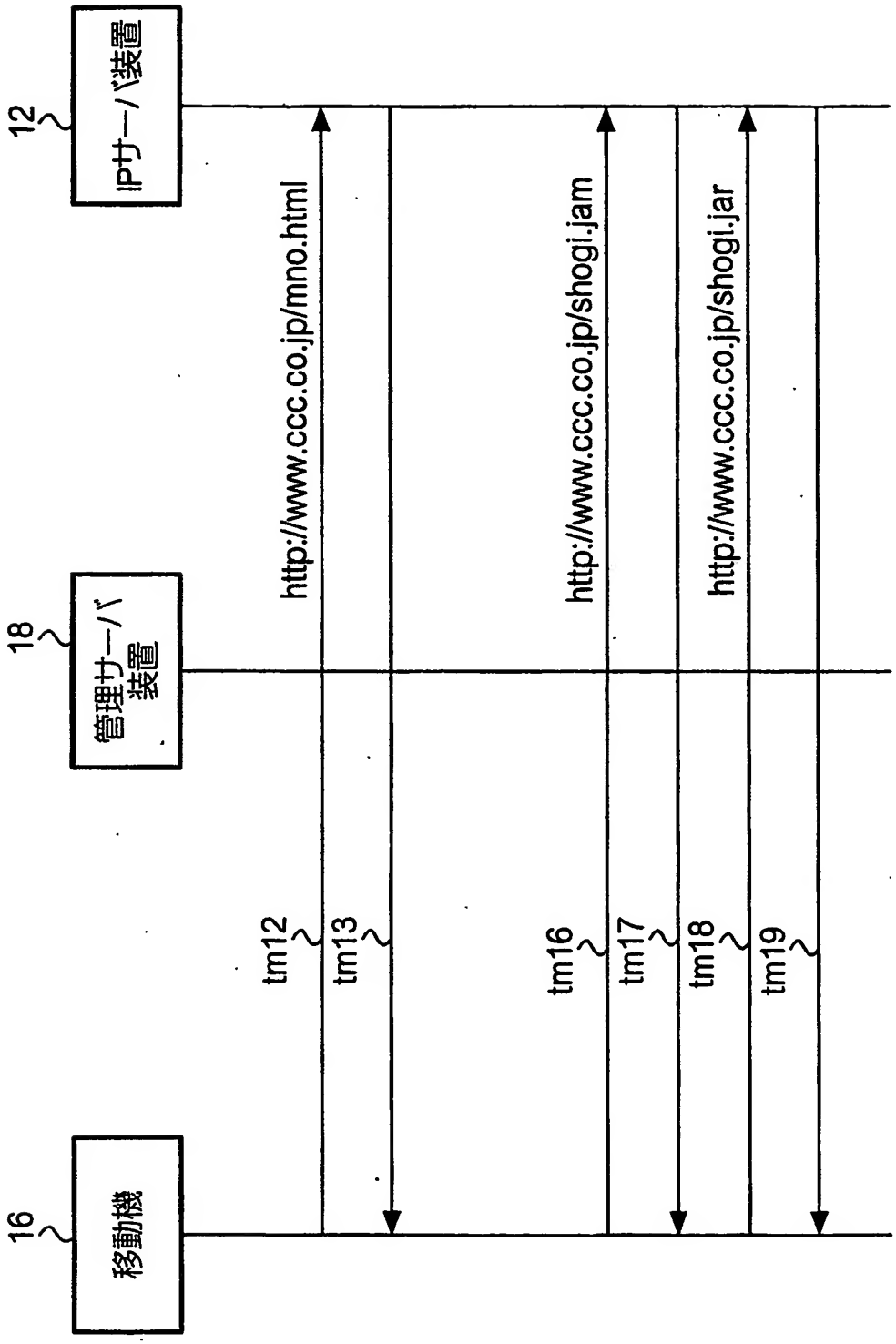
【図１４】

```
<OBJECT declare id="application.declaration"
data="http://www.aaa.co.jp/abc.sdf"
type="application/x-jam">
電話帳ビューア
</OBJECT>
　～するソフトウェアです。ダウンロードするには
<A ijam="#application.declaration">ここ</A>
をクリック。
```

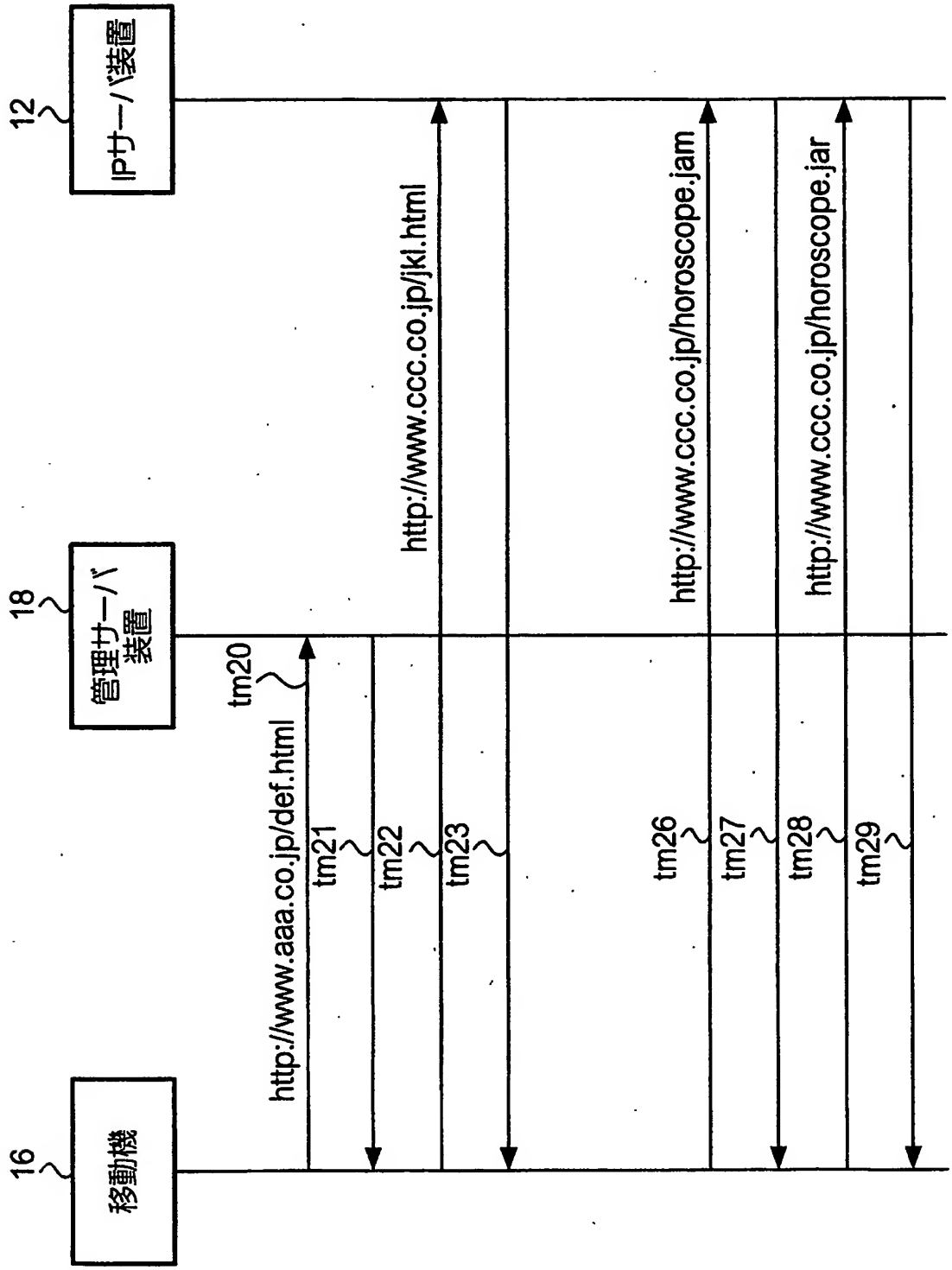
【図１５】


16C
電話帳ビューア
・・・・・・・・・・・・・・・・・・・・・・
・・・・・・～するソフトウェアです。ダウンロードするには、ここをクリックしてください。
203
203A

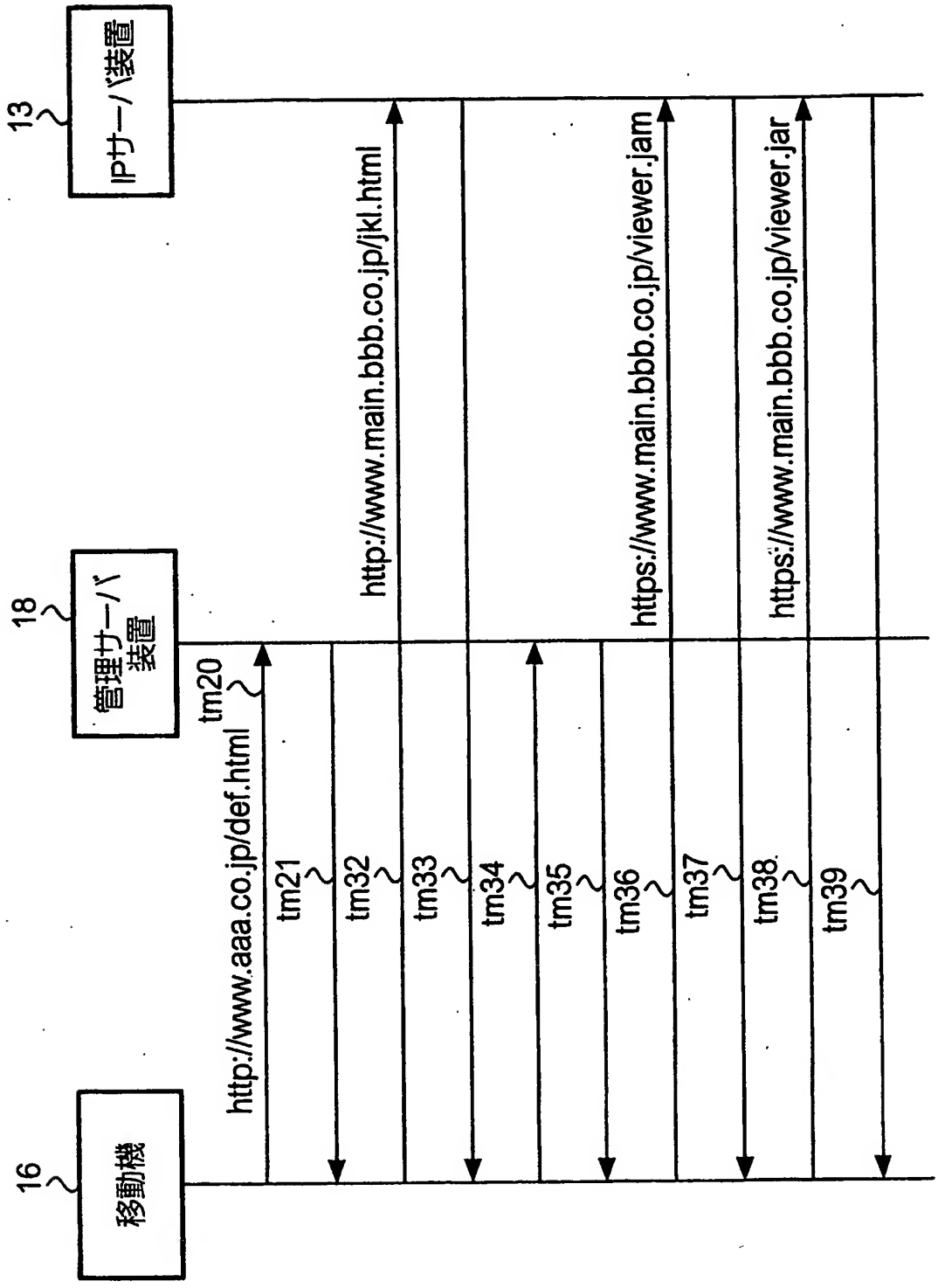
【図１６】


12
IPサーバ装置
18
管理サーバ装置
16
移動機
http://www.ccc.co.jp/mno.html
http://www.ccc.co.jp/shogi.jam
http://www.ccc.co.jp/shogi.jar
tm12
tm13
tm16
tm17
tm18
tm19

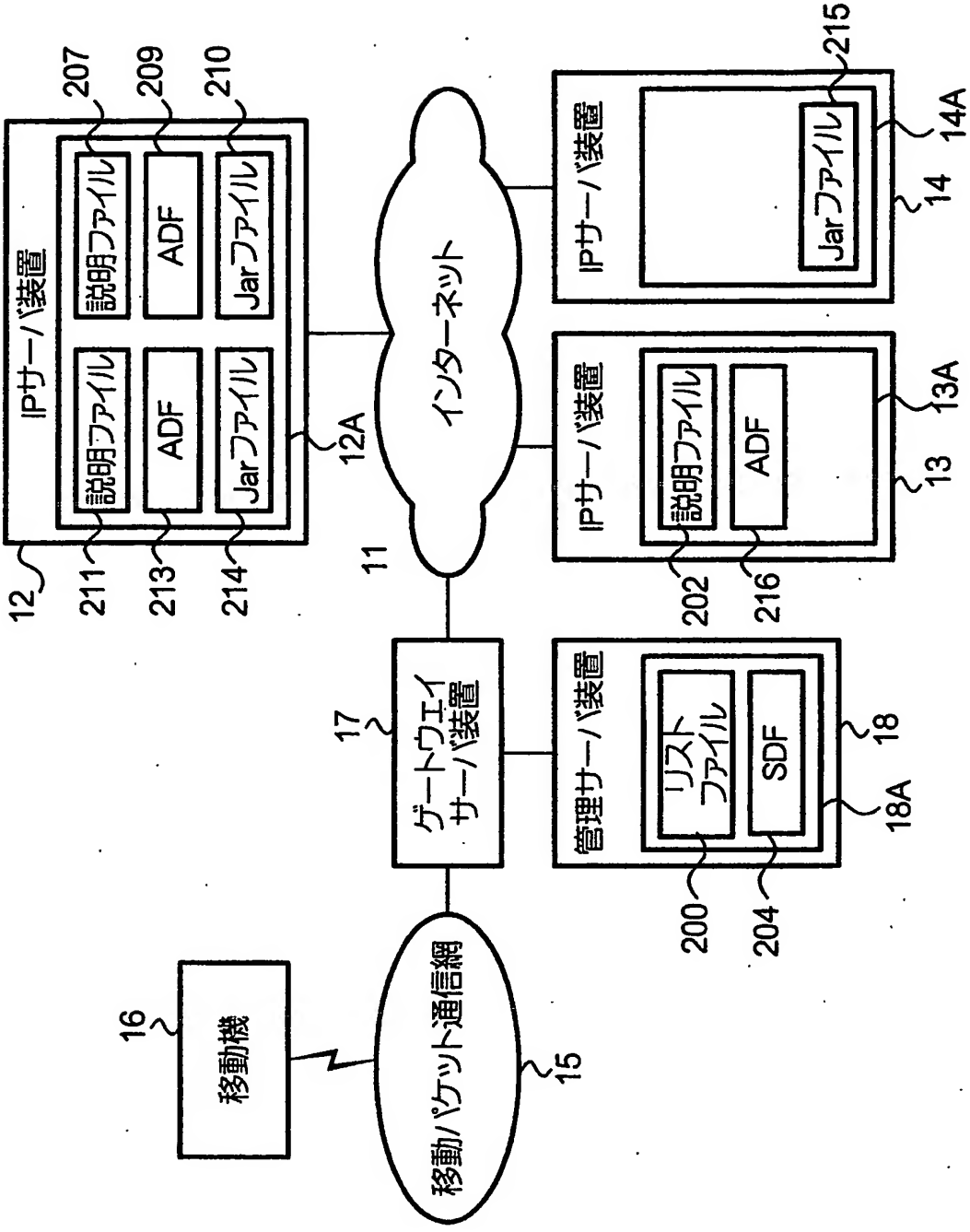
【図１７】


12
IPサーバ装置
18
管理サーバ装置
16
移動機
http://www.ccc.co.jp/jkl.html
http://www.ccc.co.jp/horoscope.jam
http://www.ccc.co.jp/horoscope.jar
tm20
http://www.aaa.co.jp/def.html
tm21
tm22
tm23
tm26
tm27
tm28
tm29

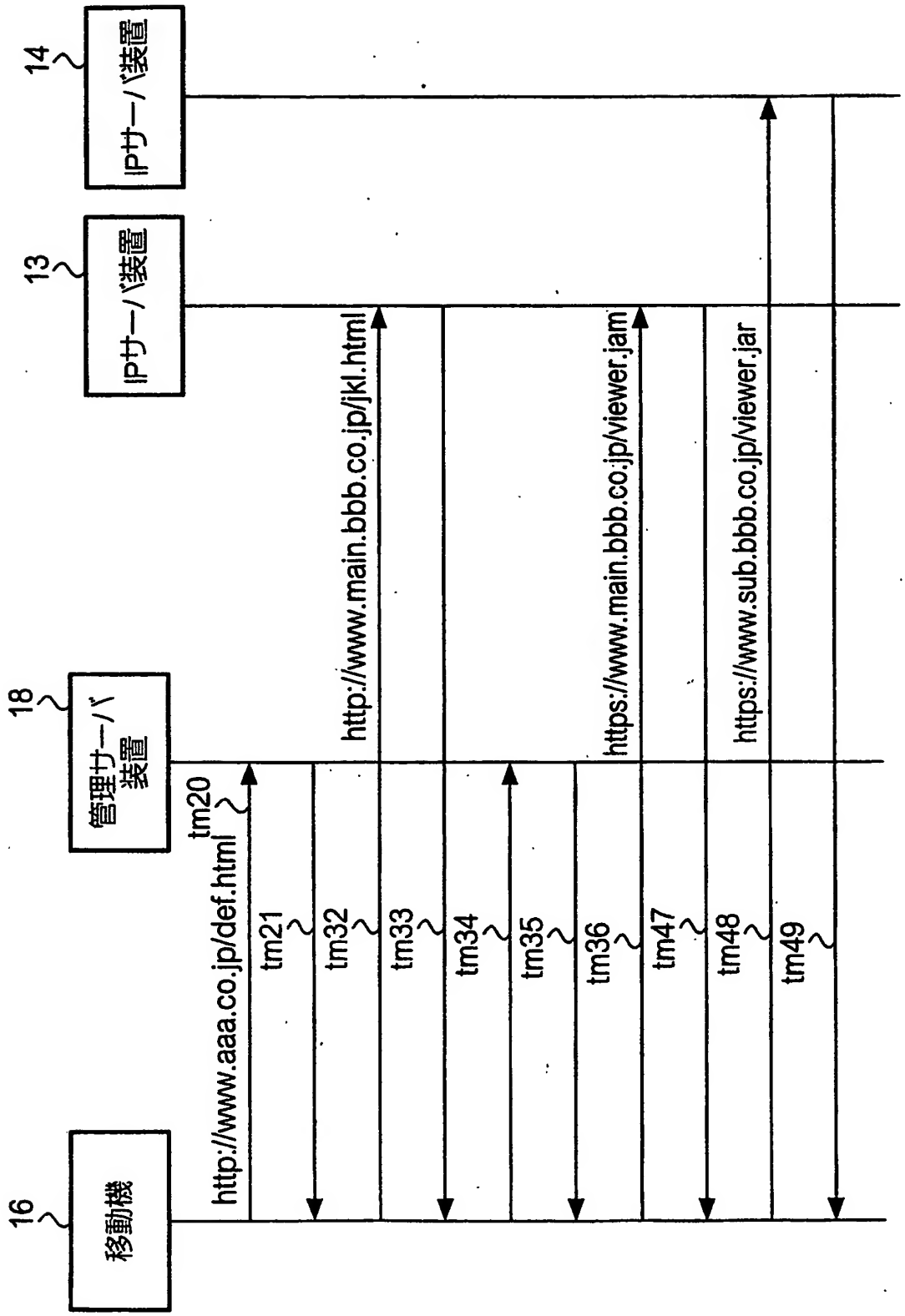
【図１８】


13
IPサーバ装置
18
管理サーバ装置
16
移動機
http://www.aaa.co.jp/def.html
tm20
tm21
http://www.main.bbb.co.jp/jkl.html
tm32
tm33
https://www.main.bbb.co.jp/viewer.jam
tm34
tm35
https://www.main.bbb.co.jp/viewer.jar
tm36
tm37
tm38
tm39

【図１９】


IPサーバ装置
説明ファイル
ADF
Jarファイル
207
209
210
211
213
214
12
12A
インターネット
11
IPサーバ装置
Jarファイル
215
14
14A
IPサーバ装置
説明ファイル
ADF
13
13A
202
216
ゲートウェイサーバ装置
17
管理サーバ装置
リストファイル
SDF
18
18A
200
204
移動機
16
移動パケット通信網
15

【図２０】


16
移動機
18
管理サーバ装置
13
IPサーバ装置
14
IPサーバ装置
http://www.aaa.co.jp/def.html
tm20
tm21
tm32
http://www.main.bbb.co.jp/jkl.html
tm33
tm34
https://www.main.bbb.co.jp/viewer.jam
tm35
tm36
tm47
https://www.sub.bbb.co.jp/viewer.jar
tm48
tm49

【書類名】　　要約書

【要約】

【課題】　ＩＰの自由度を制限することなく、信頼性の保証されたＪａｖａ－ＡＰ（Ｊａｖａアプリケーション）ソフトウェアを移動機へ配信する。

【解決手段】　Ｊａｖａ－ＡＰソフトウェアを起動することができる移動機１６が、信頼できる機関（移動パケット通信網１５を管理する通信事業者）が管理する管理サーバ装置１８からＳＤＦ（セキュリティ記述ファイル）２０４を受信し、このＳＤＦに内包されているＵＲＬを用いてＩＰサーバ装置１３からＡＤＦ２０５を取得し、このＡＤＦ２０５を用いてＩＰサーバ装置１３からＪａｒファイル２０６を取得し、これらのファイルを内包するＪａｖａ－ＡＰソフトウェアを自身にインストールする。このＪａｖａ－ＡＰソフトウェアを起動することで実現されるＪａｖａ－ＡＰは、ＳＤＦ２０４に内包されているポリシー情報で表される権限の範囲内で動作する。

【選択図】　　図８

出 願 人 履 歴 情 報

識別番号　〔３９２０２６６９３〕

１．変更年月日　２０００年　５月１９日
［変更理由］　名称変更
住　所　東京都千代田区永田町二丁目１１番１号
氏　名　株式会社エヌ・ティ・ティ・ドコモ